South Harringay School
Data Protection Policy

Member of staff responsible: Mike Gordon
Date approved by Full Governing Body: November 2021
Date to be reviewed: Autumn Term 2023

1. Policy Ownership and Responsibilities

This policy on the Use of ICT relates specifically to school employees. Governors will need to adopt this policy and implement it at school level.

The Use of ICT policy should be issued to staff as part of the documentation given to all new staff. It should be read before using any ICT services. Failure to comply with the policy could lead to disciplinary action being taken against the employee, which could lead to dismissal, and in some cases legal action.

Employees are responsible for maintaining their awareness and complying with this policy and the headteacher is responsible for monitoring compliance.

Any employee discovering a breach of this policy, or who is in receipt of an electronic mail or telephone call that appears to contravene the policy described below, should raise the issue with their line manager or headteacher in the first instance. Where the concern or issue persists and cannot be resolved the headteacher should refer the matter to the Director of Education.

An employee who is subject to and has received a copy of this policy and uses ICT services will be deemed to have consented to the monitoring and surveillance of e-mail, Internet and workstations. Monitoring will be undertaken if a breach of policy is suspected.

2. Terms Used in this Document

The following terms are used in the document:

- "**must**" means that any failure to comply is a serious breach of the policy;
- "**should**" means that compliance is strongly recommended but non-compliance may be acceptable in exceptional circumstances;
- "**electronic mail**" covers all communications stored electronically, including e-mail, voice mail and items transmitted via facsimile;
- "**document**" refers to either one or more electronic files used to record information;
- "**database**" refers to either one or more electronic files used to record information in a highly structured format;
- "**computer system**" refers to any combination of computer hardware, computer software and data that can be considered a discrete system;
- "**workstation**" refers to any desktop, portable or palmtop PC;
- "**ICT**" refers to Information Communications & Technology;
- "**employee**" refers to any permanent, temporary or part-time employee, or casual worker, at the school (agency staff and consultants **should** be covered by the same

policy in their contractual agreement);
- **"Council"** refers to Haringey Council.

3. Policy Objective
The purpose of this policy is to ensure that employees who use ICT services, including e-mail, Internet, Intranet, desktop, telephones and fax, do so in accordance with the school/council's business objectives and values. This will assist the school/council in protecting employees from inappropriate use of technology, protect the security of information held on systems and limit the opportunity for fraudulent use of technology.

The policy is also intended to set out good practice for communicating, storing and retrieving information.

4. Scope
This policy applies to all school based employees. It is based on the Corporate use of ICT policy. Relevant sections of this document should also form part of a contract for services for agency staff and consultants.

Controlled use of ICT relies on a combination of responsible behaviour by users and the implementation of security features by ICT management and system owners. The scope of this policy does not extend to the latter but refers only to the responsible use of ICT by employees.

5. General Policy

5.1 Acceptable Use
Employees **must** not use any ICT services for copying, storing, sending or retrieving unacceptable material. "Unacceptable material" includes any documents, messages, information, graphics or other electronic data that:

- breach UK legislation; contravene the school/council's Equality Policy
- contain offensive, pornographic or obscene language or material;
- plan, promote, incite or facilitate any illegal or terrorist activities;
- contain defamatory or slanderous language or material;
- denigrate, insult or ridicule another person;
- intimidate, bully or harass another person;
- adversely comment on the integrity, personality, honesty, character, intelligence, methods or motives of another person unless it is a factual response to a formal reference request;
- provide or facilitate the use of computer hacking tools or virus toolkits.

Use of such material for teaching/research purposes, which would otherwise be contrary to this policy, may be permissible at the discretion of the headteacher .

Employees **must** not use the Internet, electronic mail, telephone, or any other form of electronic communication to transmit sensitive or subversive information, including:

- opinions that do not reflect the policies of the school/council (but see section 7.3 for Facilities Arrangements exception);
- that which could prejudice the security of the school/council's assets;
- information that could damage the school/council's reputation and standing in the community.

5.2 Data Protection
The school/council both have nominated Data Protection Officers who are tasked with ensuring that the school/council records, stores and transmits data in compliance with the Data Protection Act 1998.

The Data Protection Act 1998 puts certain legal obligations on the school/council for the recording and storing of personal information. Any queries should be addressed to the Data Protection Officer.

Employees responsible for computer systems that record personal information **must** ensure that all such systems comply with the Data Protection Act 1998

Any employee who develops a database, spreadsheet or other computer system that records personal information **must** ensure that the system complies with the Data Protection Act 1998.

5.3 Intellectual Property Rights
With the facilities offered by ICT systems it is now a straightforward operation to copy, store and transmit complex information. However in doing so it is essential that intellectual property rights are respected.

Material that is Copyrighted or Trademarked, or other proprietary material **must** not be copied, stored or transmitted without the express permission of the owner. Such action, whether knowing or inadvertent, may result in liability to the school/council and/or the individual responsible.

Employees should be aware that, in general, the employer retains intellectual property rights to all material that is created by employees as part of their work. In certain circumstances the intellectual property rights may be shared, if an agreement to this effect is drawn up prior to such particular work being developed.

6. System Security Policy
The school is responsible for establishing and enforcing a password policy for its use of ICT. Application system owners are responsible for establishing and enforcing a password policy on their systems based on the level of security required.

Passwords are assigned to individual users of ICT systems for the following reasons:

- to maintain the security of systems and the data that they contain;
- to ensure that all access and modification to the data can be traced back to an

individual employee.

6.1 Ownership

All systems have a designated system owner, though this phrase is used as a convenience to describe the part of the Council or the school that has the delegated responsibility for the maintenance and integrity of that system.

Some applications have the sole system owner of Education Services, such as the intranet system. Most applications are owned by the school which pays for or maintains the system.

6.2 Securing Passwords

Employees **must** protect their passwords, as they will be held accountable for all activities undertaken under their usernames.

Employees **must** keep their passwords private and where written down must be kept in a secure location such as a safe or cash box.

Any password used by an employee **must** be provided, on request, to their headteacher, the Director of Education, the Head of Personnel, or the Council's Head of Audit, or any of their nominated officers.

6.3 Choosing Passwords

Passwords **should** be chosen in a way that makes them difficult to guess, i.e. obvious words, names connected with the user, dates or repeated characters.

For each computer system that has its own acceptable password policy, this **must** be complied with by all users of that system.

Groups of employees **must** not share the same password for their individual usernames on a computer system unless there is a valid technical and operational reason. Such action defeats the objectives of secure and accountable access to data.

6.4 Staff Changes

The headteacher will ensure that new employees are issued with appropriate usernames and passwords.
When an employee leaves their job, whether leaving the school/Council or not, the headteacher will ensure that all usernames and passwords for that employee are suspended as appropriate.

6.5 Access to Systems

Employees **must** never attempt to gain unauthorised access to other computers, networks or information either within or external to the council. In the UK this is an offence under the Computer Misuse Act.

Employees **must** not use the username and password of another employee unless the access is in connection with a formal request for the provision of a password made by the headteacher, Director of Education, Head of Personnel, or the Head of Audit, or any of their nominated officers.

Most computer systems will automatically suspend a username if repeated attempts are made

to access it using an incorrect password. If this occurs then the employee to whom this username is assigned **should** contact the appropriate system manager to have the username unlocked.

Employees **must** not give any person not employed by or undertaking an approved course of study at the school/council access to any computer system whilst that person is in school/council premises without the written permission of the headteacher/ Director of Education, or one of his/her nominated officers.

Employees **must** not subvert any system that controls or monitors access to a computer system.

6.6 System Integrity

Employees **must** not intentionally damage or compromise the integrity of any computer system.

Any computer system, data or workstation taken off school/Council premises must be protected with a security system if so specified by the headteacher/ Director of Education, or one of his/her nominated officers.

Employees **must** not alter any information held on any computer system for any reason other than the normal performance of their duties.

Line Managers **must** ensure that where data backup or security procedures are delegated to them that these procedures are followed.

6.7 Encryption

Files may be password protected where the application software has such a facility built in. Where files are password protected employees **must** make provision for line managers and/or colleagues to gain access to the file in their absence. Employees **must not** knowingly install or use any other encryption software without the written permission of the headteacher/ Director of Education, or one of his/her nominated officers.

7. Electronic Mail Policy

The school/Council provides electronic mail systems for business use. Electronic mail users **should** be aware of the importance of checking email regularly, using common courtesy in messages, performing regular housekeeping and discouraging excessive, inappropriate or wrongful use of the system.

7.1 Ownership and Privacy

All electronic mail originating, arriving, or in transit through any electronic mail system belonging to the school/council is the property of the school/council.

An employee may be granted access to use an electronic mail system at the discretion of management and the school/council reserves the right, in its sole discretion, to suspend or terminate any persons use of electronic mail at any time, for good reason. In addition the school may take disciplinary action against any person who misuses electronic mail.

The council strives to provide controls to safeguard information access to its electronic mail systems. The council reserves the right to monitor, access, review and disclose all messages without the additional consent being required from any employee, contractor, vendor or

person who uses an electronic mail system belonging to the council. Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe that a breach of this policy has occurred.

Electronic mail communications, either internally or on the Internet, are not guaranteed to be private or to arrive at their destination either within a particular time, or at all.

7.2 Private Use

The school/council's electronic mail systems **must not** be used for private use other than where agreed as acceptable within this policy.

If employees wish to send and receive private electronic mail then they **should** subscribe to an Internet based service and access this service in their own time.

7.3 Acceptable Use

As well as the general policy detailed above, the following specific usage constraints for electronic mail also apply:

- electronic mail used to complete transactions, such as transfer of funds, **must** only be used in controlled environments that can ensure the authenticity of the originating persons (for advice on this subject contact Education Information Services);
- employees **must not** use e-mail to provide any reference of a personal nature i.e. employment, medical or financial without confirming the authenticity of the request;
- employees **should not** send irrelevant or inappropriate e-mail to mailing lists;
- employees **must not** participate in chain or pyramid letters or similar schemes;
- employees **must not** use a third party electronic mail system in place of the Council's system without the written approval of the headteacher/ Director of Education, or one of his/her nominated officers;
- employees **should** report to their line manager, or such other appropriate officer, the receipt of any e-mail that they consider to be offensive or that may be construed as bullying or harassment;
- messages **should** be communicated in a way that clearly identifies the author and if writing to someone that isn't known to the author then they should include their first name, surname, job title, and if relevant, the organisation;
- an employee receiving an electronic mail message in error **must** inform the sender immediately and delete the message from the system;
- trade unions/professional organisations should use ICT in accordance with the Facilities Agreement.

7.4 House-keeping

The headteacher/Director of Education should set a maximum size for an electronic mail box and where possible ensure that the system enforces this automatically. The headteacher/Director of Education may periodically delete all messages older than a certain date or larger than a certain size. Where possible notice will be given that such deletions are to occur but this may not always be possible.

Employees **must** reduce the size of their mailbox if requested to do so by the headteacher/Director of Education,or one of his/her nominated officers.

Employees **should** check their electronic mail on a regular basis.

Employees should arrange to set up a rule notifying other users sending messages when they are on leave for more than 2 days. The return message should state an alternative contact who can deal with work in their absence.

Large attachments **should** be saved from the e-mail, and the mail message containing them deleted so as to reduce the storage requirements of the electronic mail systems.

7.5 Good Practice Guidelines

The following good practice guidelines **should** be observed:

- e-mail is intended for business use and whilst correspondence is generally briefer than other correspondence, try to use correct grammar and spelling making use of the spell checking facilities on the e-mail system;
- consider the correspondence to be permanent and do not assume that the e-mail, when deleted, will be lost forever;
- take care when communicating sensitive information;
- take care when communicating with someone in another country as insensitive use could lead to litigation in that country;
- training on the use of ICT should be offered to all appropriate employees;
- keep a permanent record of an e-mail containing substantive advice;
- do not communicate information via e-mail that you would not be prepared to say to the recipient if you were talking face to face;
- avoid inappropriate use of upper case in e-mail as it is generally interpreted as shouting;
- wherever appropriate, other people's comments or observations should be communicated verbatim by using the "threading" capability of e-mail i.e. using Reply and Forward options so that the message history is retained (do not quote comments or observations from other people as a quote may be taken out of context);
- care should be taken to address electronic mail to the intended recipient as misaddressing is common;
- clearly title messages so that the contents can be understood before the message is opened;
- clearly mark a message "for information" if no action is required;
- make it clear what action or response is required from each recipient;
- do not copy or forward unnecessary messages to others;
- the approval of the headteacher/principal should be sought prior to searching any web-sites which would normally be deemed inappropriate.

7.6 Education Intranet

The council provides on line discussion facilities for business usage. These facilities are maintained by the Council's nominated officer and he/she may delete any message on any discussion forum at his/her discretion. School-based moderators may delete messages in the particular discussion forums for which they hold responsibility.

Employees should not post messages to discussion forums that are not relevant to the usage of that particular forum. Where doubt exists as to the usage of that particular forum, then messages should not be posted.

8. Internet Policy

The school/council's objectives in providing Internet facilities is to facilitate teaching and

learning, to help facilitate business objectives and meet e-government targets.

8.1 Access
The school/council provides a secure, filtered and monitored Internet feed, access to which may be granted to a member of staff at the discretion of their management.

Employees **must** not attempt to bypass the security, filtering or monitoring services on the Council Internet service.

Employees must not access any unsuitable material that is not filtered.

8.2 Ownership and Privacy

The school/Council reserves the right to monitor, access and review an individual's use of the Internet without the additional consent being required from any employee. Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe that a breach of this policy has occurred.

8.3 Private Use
An individual may request the private use of the Internet under the following circumstances:

- private use must be approved in advance by the employee's line manager including the length of time that it may be used privately;
- private use **must** only occur in the individual's own time (outside of contractual hours);
- private use must comply with this policy on the use of the Internet.

8.4 Downloading
Employees **must not** download or install any programs from the Internet on to the school's network without the permission of the headteacher or one of his/her nominated officers.

9. Workstation Policy
Workstations are provided by the school/Council for business use and must not be used for any other purpose other than where agreed as acceptable within this policy.

9.1 Ownership and Privacy
All programs stored on a school/council owned computer are the property of the school/council and not individual employees.

An employee may be granted access to use a workstation at the discretion of management and the school/council reserves the right, in its sole discretion, to suspend or terminate any persons use of any or all workstations, at any time. In addition the school may take disciplinary action against any person who misuses workstations or systems accessible through it.

The school/council reserves the right to monitor, access and review an individual's use of workstations without the additional consent being required from any employee. Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe that a breach of this policy has occurred.

Every workstation has a designated person responsible for its use, for the software resident in

the machine and for compliance of this policy. This person will be one of the following:

- the occupant of the desk on which the machine resides;
- the manager of an area where workstations are a shared resource for a group of users;
- a user allocated a workstation on a temporary or permanent basis.

Headteachers/ line managers **must** retrieve school /council owned hardware, software and equipment from employees, contractors and temporary staff leaving their employment.

9.2 Private Use
Workstations **must** be used only for school/council business and must not include;-

- processing relating to commercial activities;
- any activities that could potentially reduce the security of school/Council systems and data;
- creation of non employment related private intellectual property;
- saving of any non -employment related data to a network drive.

9.3 Off-site Use
The following procedures apply where an individual requests the use of ICT hardware off-site:

- the individual **must** seek authorisation from their line manager stating the nature and duration of use;
- the employee and their line manager **must** sign a document stating the item of equipment, serial number or other relevant identification, the date that the equipment was taken from the school/council's premises and the duration that it will be off-site;
- the employee and their line manager **must** sign a document stating the date that an item of equipment is returned to the school/council's premises;
- the employee accepts responsibility for the equipment once it has been signed for;
- the headteacher or designated employee **must** be informed on the first occasion that an item of hardware is used off-site and the documents referred to above must be made available for his/her inspection as required;
- the school is responsible for securing appropriate insurance for all equipment used off-site.

9.4 Software
The software installed onto workstations is very tightly controlled and this may be done by the use of automatic control software installed on the workstation. The following restrictions apply to all software:

- all software installed **must** be properly licensed; the use of all software **must** comply with the conditions of the relevant licence agreement;
- all software installed **must** be relevant to the work of the operator of that workstation or the team or department in which it is based;
- free, public domain or shareware software is subject to the same restrictions on use as all other software and **must** only be installed in compliance with this policy;
- employees **must** not attempt to circumvent any security system installed on a

workstation by management, this includes, but is not limited to, remote control software, automatic control software, lockdown software and antivirus software.

10. Telephones/Fax Policy
The telephone and fax facilities are designed for business use only. Personal use is only permitted in the following circumstances:

Either the call is in the London Area
or

- authorisation has been sought from the employee's line manager, and the call is urgent and could not wait until an appropriate work break;
- the call is connected with the employee needing to work later than expected;
- the employee reimburses the cost of the call, other than calls in connection with the employee working late.

Employees **must** not use the school's telephone system or their own personal mobile phones to receive private calls whilst working unless the call is urgent.

The school/Council reserves the right, in its sole discretion, to suspend or terminate any person's use of any telephone or fax equipment at any time. In addition the school may take disciplinary action against any person who misuses the telephone system.

Telephone lines **must** not be connected, to any equipment, other than to a fax machine, without the permission of the headteacher or one of his/her nominated officers.

The Headteacher **should** ensure that all school fax machines are registered with the appropriate service to avoid receiving 'Junk' faxes.