Waverley Primary School

ICT – Information Security and Acceptable Use Policy

1 Scope

This policy applies to:

- All staff users of School's information systems, including but not limited to employees, contractors, consultants, external auditors, student teachers and temporary staff, including those from private Supply Agencies.
- All School's information whether held on paper, film, fiche or electronically, and ICT equipment, including computers, servers, printers, telephones and hand-held devices such as PDAs and 'smart phones'.
- All School owned ICT assets including but not limited to Laptops, Desktops and PDAs (personal digital assistant).
- All School's data and all reports derived from such data.
- All programs developed by School employees or on behalf of the School, using School equipment or personal computers used for home working by School employees.
- All communication lines, and all associated equipment or devices used on School premises or connected to School resources that are capable of processing or storing the School's information.

This policy does not cover pupils within schools, adult learners or parents. The ICT Managed Service will work with any school to produce an appropriate security policy to cover these groups if one does not already exist.

2 Purpose

This document deals with guidance for School Staff primarily in the areas of information security and acceptable use.

It is recognised that schools maintain a level of freedom as to how they operate their institutions; as such this document represents the recommendations of the managed service produced in line with guidelines laid out in ISO 27001:2005 and other industry best practice including Becta, the Information Commissioner's Office and DCSF advice.

The ICT Managed Service and HR Services will work with all schools to support them through implementing the guidance set out in this document.

The ICT Managed Service and HR Services are committed to supporting the protection of the security of Schools information through the preservation of:

- **Confidentiality** - protecting information from unauthorised access and disclosure.
- **Integrity** – safeguarding the accuracy and completeness of information and processing methods.
- **Availability** – ensuring that information and associated services are only available to authorised users when required.

3 Roles and Responsibilities

Governing Body: The Governing Body has overall responsibility to ensure that the procedure is properly and fairly applied.

Head Teacher: The Head Teacher is responsible for ensuring that all staff are aware of this policy and comply with the guidance

4 Policy Aims

The aims of this Information Security policy are:

- To ensure that all information and information systems on which the School depends are adequately protected to the appropriate level. This includes ICT infrastructure for the retrieval, sharing and dissemination of business critical data and conducting daily transactions.
- To ensure that all staff and other users are aware of their responsibility for the security of School information.
- To help staff use information more securely.
- To ensure that all staff and other users are aware of their responsibilities for processing personal information under the Data Protection Act 1998.
- To ensure that all staff are aware of their accountability and that they are aware that failure to comply with the Information Security Policy is a disciplinary offence. Any action taken will be in accordance with the relevant School or Council disciplinary procedures.
- To ensure that information assets, computers and communication systems that are owned by Schools and supported by the Managed Service are protected against external and internal threats.

5. Guidance

Staff members represent a key component in the delivery of information security and a secure environment. Investment in secure technology and secure processes is meaningless unless all staff are aware of the role they need to play in security and what is acceptable.

The following section outlines areas of personal responsibility for staff members and is intended to provide clear guidance as to the expected role of school staff in providing and maintaining a secure ICT environment in Schools.

The Managed Service will work with all schools and individual staff members to provide any clarification, training or support that is required to ensure that everyone understands their roles and responsibilities.

5.1 Security Awareness Training

In order to ensure that staff fulfils their responsibilities for ICT and Information Security it is essential that appropriate training is provided to ensure an awareness of the legal and procedural expectations placed upon them.

To this end, the ICT Managed Service will offer Security Awareness Training to all existing staff, and to all new members of staff in the form of induction training.

Security Awareness to staff will cover the following key areas:

- Known threats, risks and implications
- Acceptable Use
- Password Guidance
- All staff members will be trained and made aware of their personal responsibility for maintaining information security and their roles in the classification process.
- Awareness of this document and any other relevant School policy documents.

5.2 Acceptable Use

This section is intended to provide staff members and users of ICT in schools, with guidance on acceptable and unacceptable use when using information and the Information and Communications Technology (ICT) facilities provided by Schools and supported by the Managed Service.

If you have any questions or concerns then please contact the ICT Service Desk.

Further practical advice on acceptable use can be found in the following Becta Document.
Becta Do's and Don'ts

5.3 Investigations

If there are any concerns that the policies or guidance within this document have been breached, or there is a suspicion of criminal activity then this must be escalated directly to a member of the Schools Senior Management Team. They will then communicate directly with the Senior Management of the Managed Service and Human Resources to discuss any investigation that may be required.

Further specialist advice may be sought from the ICT Security Team or the Information Governance Team.

5.4 Using computer equipment

Each user is responsible for the workstation that they use; the data it holds and the output produced. This also applies to portable equipment, media or data that is used away from the normal place of work.

You **MUST**:

- Keep any portable equipment securely, and carry it safely; lock it away if you leave it in the office overnight
- Keep Remote access or ContactPoint tokens safe at all times and report their loss immediately.
- Unless instructed otherwise, log off from the network every night and switch off the PC
- Connect portable computers to the network at least once a month to keep the anti-virus and patching protection up to date
- Report any problems as soon as possible to the ICT Service Desk including the loss of, or damage to, any ICT equipment.
- Ensure that any redundant ICT assets are disposed of in a secure and legal manner. The Managed Service can support schools in this process to ensure that the correct information is recorded and that any equipment is disposed of in a secure manner. The Asset Transfer section covers this information in more detail.

You **MUST NOT**:

- Connect any non school ICT devices to the network without the permission of Senior Management and the involvement of the Managed Service. This also applies to equipment brought in by your visitors, including students, presenters, trainers and consultants.
- Allow students to logon to your laptop or desktop machine
- Allow students to use a machine logged on using your or another persons username and password.
- Logon to a student workstation without the prior permission of a member of the SLT.
- Move any computers equipment, printers etc without informing the Managed Service.
- Save any information on to any computer or device which is not registered as School equipment.
- Change any computer programs or settings. Note that this does not include printer settings which you might need to change to use the printer.
- Change any folder or file's permissions in a way that prevents people from accessing information that they are entitled to see.

You **SHOULD**:

- lock your PC screen using Ctrl / Alt / Del then "Lock Computer" (if available) whenever you are away from your desk, to prevent someone accidentally or deliberately looking at information, making unauthorised changes, or sending email in your name
- Logout if you are going to be away from your machine for any length of time.
- Report any instances of possible security breaches, including near misses. For example if
    - a colleague is using someone else's log-in name and password
    - you can see personal information on a computer screen in an unattended area

5.5 Passwords

Effective username and password combinations are a basic security requirement for any information system, but they are only effective if used properly.

You **SHOULD**:

Choose a password that:

- Is at least 8 characters long
- Contains at least one letter and at least one numeric character
- Contains both uppercase and lowercase letters and at least one punctuation mark or other “special character”
- Where the system cannot meet these requirements you will use the maximum complexity that the system allows
- Change your password at least every 90 days
- Change your password as soon as possible, if anyone else gets to know it. Help and support is available through the Managed Service to support this process

You **MUST NOT**:

- Disclose your password to anyone else
- Use another person’s logon name or password, or
- Allow someone to use another person’s logon name and password
- Use another person’s machine whilst they are not there if they have not locked it (log the machine off or lock it for them).
- Not use the same password twice
- Write your password down and keep it where anyone else may be able to read or use it
- Reply to any email asking for your username, log in details or password (even with a refusal, since this lets the sender know that they have located a valid email address)

You **SHOULD**:

- Follow the guidance on permissions. If another member of staff has a **legitimate business** need to view your email account while you are away from the office, you should, unless there are unforeseen circumstances, set this up before access is required. Please contact the ICT Managed Service for advice and support to help you through this process.

5.6 Saving files

In order to keep the School's information secure, you should not use the c: drive to save any work related files.

You **MUST**:

- Save files on to the server rather than on to your PC
- Save files to appropriate locations on the network
- Restrict access to strictly confidential information on a need to know basis. Help and support is available through the Managed Service to support this process.

You **SHOULD**:

- Save your file every few minutes as you work on it.

You **MUST NOT**

- Keep any information on a PC in an area where it is particularly vulnerable to theft.

5.7 Using Internet and E-Mail Facilities

All network users have access to the Internet, e-mail and calendar. By accepting your network account password and related information, and accessing the network, you agree to keep to this policy. You also agree to report any network misuse to the ICT Service Desk and your Line Manager. Misuse includes policy violations that harm another person or another individual's property.

The Internet, Email and calendar systems are provided for business and curriculum purposes. If you are unsure whether an activity constitutes suitable use, you should consult your line manager.

5.8 Personal responsibility

- Access to the Internet, email and calendar during working hours shall be through a school device attached to the network.
- E-mail access is also permitted via the webmail portal or an authorised mobile device.
- Staff should only access approved e-mail systems within school, such as the schools exchange e-mail or authorised VLE solutions.
- It is essential that communications with students are in connection with teaching and learning. Staff should only use their official school e-mail addresses when communicating with students
- Work related information must not be communicated on non school e-mail systems. The security of the data can not be guaranteed.
- If other staff need to access your email account (for example, during leave or sickness) you should consider giving them access through the 'permissions' facility on the email system. Help and support on this area is available through the Managed Service.
- No information should be sent via e-mail which is prohibited by the Information Asset Classification section of this document. If in doubt please consult your line manager or the Managed Service.

5.9 Personal use

- Personal use of any ICT resource must not involve any unacceptable use.
- Personal email conversations in work time must be as short as possible and kept to a minimum. Personal use of the Internet is allowed outside of working time, for limited periods or at other times with your Manager's approval.
- You should ask your line manager if you are in doubt about the acceptability of any personal use. Access to any ICT facilities may be removed or disciplinary action conducted by your employer if you are found to be misusing resources.
- Use of social networking sites may be appropriate on occasions for professional reasons e.g. contact with colleagues in other schools, but we strongly recommend that staff members do not allow access to their own personal areas or open lines of communications to students via social networking sites. It is very important that staff members maintain professional relationships with students at all times and we feel that these may be compromised by allowing students access to personal information or photographs. If you do have any students (including Post 16 students) as contacts please remove them to protect yourselves as professionals.

5.10 Unacceptable use

Any use of the internet or ICT facilities which is against any relevant legislation or any internal school policies is unacceptable and could lead to disciplinary action. If you are in any doubt about any use, you should contact your Line Manager.

Examples of unacceptable use include:

- Using 'chat rooms' and 'discussion forums', or for circulating jokes, personal photographs or malicious comments about other people on 'social networking sites'.
- Deliberate access to or sending any material that is against any of our policies.
- Illegal or malicious use, including downloading or sending copyright material.
- Any form of online harassment (or cyberbullying), including harassment by volume of communications on 'chat rooms', 'discussion forums' or 'social networking sites', or sending 'spam'.
- Creating material, containing false claims of a deceptive nature.
- Use for private business purposes.
- Any form of gambling.
- Downloading or distributing pirated software or data.
- Revealing yours or someone else's personal information, such as, home address, telephone number, or financial data.

(This list is not exhaustive)

- Where possible, the ICT Managed Service will prevent access to material known to be of an offensive or undesirable nature using security tools and filtering software.

- If you receive an email or access a website which you consider to be offensive or potentially illegal, you must report the matter to your line manager or the ICT Service Desk.

- If you receive an email that you consider to be spam, you should forward it to education.it@newcastle.gov.uk and we will then be able to block future incoming emails from that address.

5.11 Personal information

The term 'personal information' refers to any information that in combination identifies one person to another. This could be a name, address, National Insurance or telephone number. It could also be the type of job they do, or the name and location of the school they attend.

- You should take care when sending personal information electronically, this includes uploading or sending information to an Internet site.

5.12 The security of external communications cannot be guaranteed

- Where you have an authorised business need to electronically send sensitive or confidential personal information; which relates to pupils; clients or staff, you must refer to the Information Asset Classification Policy.

If in doubt please consult your line manager or the Managed Service.

5.13 Remote Access

School Staff

- Virtual Learning Environments (VLE's) - Access to school based information away from School is achieved for many schools through the use of VLE's. It is essential that information uploaded to these environments is appropriate for such a storage mechanism and is inline with the guidance within the Information Asset Classification Policy.

- Access to email away from the office is available to all staff through Webmail

- Staff members who utilise mobile equipment, whether it be laptops, desktops, PDA's etc away from the School should operate them to the same acceptable use standards as any other school ICT equipment as if they were in school.

- You are personally responsible for keeping any work related data stored on any mobile equipment safe and secure in accordance with the Information Asset Classification section of this document. This includes but is not limited to laptops, USB devices, Mobile Phones and Cameras.

Third Party Remote Access

- Third Party suppliers and vendors that require access for support reasons must also utilise the corporate remote access solution. This access also requires that they agree to the corporate Trusted Third Party (TTP) and Non Disclosure Agreements (NDA).

6. Monitoring

The ICT Managed Service will if requested facilitate the monitoring of Internet and E-mail facilities and their usage, on behalf of all Schools to highlight non-compliance. This monitoring will include, but will not be limited to:

- all Internet sites staff browse

- all transactions staff make via the Internet

- all files downloaded or uploaded to or from the Internet

- All e-mails sent and received

- All attachments sent and received.

Therefore staff should not expect privacy on any e-mails that are sent or received, or websites visited.

Logs are retained on all e-mails that are sent and received as well as all websites that have been browsed by any user.

We may be required to disclose any information kept on computer systems to outside parties or to law enforcement authorities. This would always happen in consultation with the School Senior Management.

7. Sanctions

Failure to comply with any of the requirements of this policy may result in further action being taken by your employer in line with the appropriate disciplinary policy.

Instances of non-compliance with this policy shall be identified, documented and escalated. Remedial measures shall be implemented by the Managed Service and School SMT as quickly as possible. Deliberate non-compliance by individuals, whether they are system administrators or other users, shall be treated as a disciplinary offence.

Violations of established security procedures and inadvertent and deliberate compromise of School proprietary and personal information are actions that are adverse to the security of a School and as such may warrant disciplinary action based on the severity of the incident.

8 Relationship with other policies and procedures

- **Code of Conduct:** This sets out the standards expected of staff.
- **Disciplinary Procedure:** Schools must follow their disciplinary procedure where it is appropriate to take such action against an employee.

9 Monitoring and review

Feedback is encouraged from governing bodies and head teachers on the effectiveness of this policy and procedure.

It will be reviewed on an annual basis to ensure it is appropriate in light of recommended best practice and complies with statutory regulations. In the event of any conflict with statutory regulations, the legal provisions will have precedence over this procedure in all cases.

Governing bodies should monitor the application of this policy and procedure, particularly to ensure that their practices comply with it .

Reviewed: September 2019
Next review: September 2020