GILLINGSTOOL PRIMARY SCHOOL

Inspire ~ Believe ~ Achieve

INFORMATION ACCESS AND SECURITY GUIDANCE

Signed ...

Name: Dave Llewellyn

Chair of Governors

Date: January 2024

Signed .....

Name: Caroline Carter

Headteacher

Date: January 2024

Purpose

This information access and security policy provides clear direction and support for information security that is applicable to all staff at all levels of the organisation. The policy describes the means by which the school aims to preserve confidentiality, integrity and availability of data.

Confidentiality: information is accessible only to those authorised to have access

Integrity: safeguarding the accuracy and completeness of information

Availability: ensuring that authorised users have access to information when required.

It is acknowledged that the school has legal, statutory and contractual requirements with which it must comply. The school complies with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act.

The senior manager in the school allocated overall responsibility for information security is: The Headteacher.

Specialist security advice will be sought where necessary. South Glos LA and will be consulted as a source of such advice, for example for data protection or network security issues.

Organisational security

Each "information asset" (e.g. information system, database, etc) has an owner who is responsible for its day to day security. Information is classified according to its degree of sensitivity and confidentiality, indicating the need and priority for its protection and is labelled appropriately. Each classification has defined procedures for copying, storage, transmission (e.g. post, fax, email, telephone) and destruction.

Authorisation level	**Names of Key Personnel**	**Authorised to:**
1	All Staff	Access 'curriculum' PCs, email and internet facilities, Arbor - basic
3	Deputy Head (DH)	Access 'curriculum' and 'admin' PCs, passwords, email, Web-site construction, Arbor admin, databases
4	Head Teacher (HT) School Business Manager (SBM)	Access all information assets and data bases including 'curriculum' and 'admin' PCs, Arbor admin, email, internet, all passwords and Web-site construction

Information Asset	Purpose	Sensitivity Level	Keeper	Authorisation Level
SIMS	School data, finance	High	SBM	3
Admin PCs	Accessing Arbor	High	HT	3
Website Construction	Creating School Website – info and reporting to parents, celebrating work,	Medium	SBM	2
Hub, Router	Internet access	Low	SBM	2
Curriculum PC	Curriculum support	Low	TLR Leader	1
Internet	Curriculum support	Medium	SBM	1
email	Curriculum support, communication, info	Medium	SBM	1

Software And Physical And Services Assets	Purpose	Keeper
All software (Packaged & installed South Glos)	PC Operating Systems, admin and curriculum software	South Glos LA
Arbor	Administration, finance, assessment, communication/records	SBM HT
Digital Cameras	Curriculum support, Communication/records	Class Teachers
Photocopier, Phone	Admin & Curriculum support	SBM

Personnel security

This is the overall responsibility of the Headteacher.

Security in Job Responsibilities

Security responsibilities are clearly documented and, where appropriate, addressed at the recruitment phase and included in contracts of employment. Personnel screening processes for permanent and temporary staff include appropriate controls (e.g. availability of satisfactory references, confirmation of claimed academic and professional qualifications and DBS (Disclosure and Barring Service) check). Staff sign a Staff Confidentiality Agreement (Appendix I) as part of their initial terms and conditions of employment. There is a formal disciplinary process for employees who violate security policies and procedures and employees are made aware of the action to be taken if they disregard security requirements.

Information Security Education and Training

All staff receive appropriate training and regular updates in security policies and procedures before access to systems is granted. (Information Security Training Programme - Appendix II) This includes training in security requirements, controls and legal requirements, as well as in the correct use of information systems (e.g. log-on procedures).

Responding to Security Incidents and Malfunctions

A procedure exists for reporting and responding to security incidents, malfunctions and weaknesses. (Security Incident and Malfunction Procedure – Appendix III) All staff members are aware of their responsibilities to note and report such incidents through the proper management channels as quickly as possible. Recovery is carried out only by appropriately trained and experienced staff. Users are made aware that they should not under any circumstances attempt to prove a suspected security weakness as this could be interpreted as potential misuse of the system

Physical and environmental security

This is the overall responsibility of the Head Teacher and additionally the Deputy Head, Site Manager and Key Holders. Site security is also the responsibility of New Siblands Special School who have three SLT keys.

Secure areas

Areas in which critical or sensitive information is processed are physically secured to prevent unauthorised access, damage or interference. Control is achieved by conventional security procedures - doors and windows locked when unattended, intruder detection systems monitored 24 hours.

Equipment Security

Equipment is sited or protected to minimise the risk of theft including security marking, damage (e.g. fire, water, impact). Computers sourced through Integra IT are fitted with tracking devices to enhance security protection. Cabling has been installed as an integral part of the New Build (open Sep 2010) and is protected from interception or damage by use of conduit, avoidance of public areas, routed in roof space and away from communications cables where possible. Equipment is correctly maintained and serviced by authorised personnel/companies….

- South Gloucestershire ICT Dept. (Admin. Computer & Network Supplier)
- Photocopier - Lanier
- Telephone System – Apollo Technology

Off-site security

Equipment is not taken off-site without authorisation. Where necessary and appropriate, equipment is logged out and backed up by the School Business Manager. Equipment and media taken off the premises is not left unattended in public places. Portable computers are carried as hand luggage and disguised where possible when travelling. Home working is subject to all school requirements.

Secure Disposal Or Re-Use Of Equipment

Appropriate arrangements are made for the secure disposal of media containing sensitive information.

Confidential paper documents are securely disposed of by shredding. Storage devices containing sensitive information are destroyed or securely overwritten (rather than using the standard delete function) prior to disposal. Equipment containing storage media (e.g. hard disks) are checked to ensure that sensitive data and licensed software have been removed or overwritten prior to disposal or re-use.

Clear Desk And Screen Policy

Paper and computer media are stored in suitable locked cabinets where appropriate. Sensitive printed material is cleared from printers immediately and shredded. Business critical information is held in a fire resistant safe or cabinet. All areas of the building are covered by a sprinkler system to prevent the spread of fire.

PCs and printers are not left logged on when unattended and are protected as appropriate passwords when not in use. Users terminate active sessions and log off when finished. Where appropriate, PCs shut down or time-out after a period of inactivity, with a limited time-out facility afforded by password protected screen savers.

Communications And Operations Management

This is the overall responsibility of the School Business Manager

Protection Against Malicious Software (Viruses, Etc.)

Software licensing requirements are complied with and the use of unauthorised software is prohibited. Anti-virus detection and repair software is installed and monitored by South Glos. Electronic mail attachments and downloads and any files of uncertain origin on electronic media or downloaded are checked for malicious software before use. Appropriate business continuity plans for recovery from attack are in place (e.g. data and software is sorted and backed offsite, centrally by South Glos)

Housekeeping and Network Management

Backup procedure – all data	Nightly Back-up	Remote – South Glos
Web-site	Hosted offsite	Creative Den

Electronic Mail

Guidelines exist on when to use and not to use email. Staff members understand the potential difficulties of the difference between electronic and traditional forms of communication (e.g. speed, message structure, degree of informality and vulnerability to unauthorised actions and attack - interception and viruses). Staff members understand their responsibility not to use email in such a way as to compromise the good name of the school (e.g. defamatory email, harassment, unauthorised purchasing). (E-mail Guidance for Staff – Appendix IV)

Access control

This is the responsibility of the Headteacher.

User Registration

Formal procedures are in place to control the allocation of access rights to information systems and services. Users have authorisation from the system owner and the level of access is appropriate for the purpose. User access rights are regularly reviewed; access rights of leavers are removed immediately and redundant user IDs removed. Privileges associated with each system and user are identified, allocated on a need-to-use basis and kept to a minimum

User Password Management

Users understand the need to keep passwords confidential and to avoid sharing them, keeping a paper record or recording them in a way that makes them accessible to unauthorised persons. Passwords will be changed at regular intervals or if there is a possibility that security has been compromised, according to a system that ensures use of quality passwords. The Headteacher is responsible for selecting and advising staff passwords as appropriate. The School Business manager will implement Arbor passwords to be selected by staff with approved access, only when access is granted.

Systems Development and Maintenance

This is the responsibility of the Headteacher. Security issues are identified and considered at an early stage when procuring or developing new information systems. Input data is validated to ensure that it is correct and appropriate. Outputs and downloaded or uploaded data are checked for validity and integrity.

Pupil Use Of Systems

The school subscribes to the NAACE acceptable use policy. Parental consent is obtained for use of pupil images on the Internet (Appendix V). Pupils are introduced to safe internet use (see Acceptable Use / Computing and E-Safety Policies) and E-Safety Week is revisited through the curriculum each term.

All ICT and Internet activities will be supervised by an adult at all times. No pupils will be allowed unsupervised computer or Internet access.

Staff Use of Systems

This is the responsibility of the Headteacher

The school has an Acceptable Use policy. Additionally all staff are required to sign an Acceptable Use Policy. which outlines acceptable use and sanctions as agreed by the Council and Teaching Unions for misuse of equipment, e-mail and the internet.

Intellectual Property Rights (IPR)

Appropriate procedures are in place to ensure compliance with legal restrictions in the use of material in respect of which there may be IPR, such as copyright, design rights or trademarks. Software is usually supplied under a licence agreement that limits the number of copies that can be made of the software. Controls are in place including: maintaining an appropriate inventory or asset register of software, maintaining proof of licence ownership (e.g. licences, master disks, manuals, etc), controlling the number of users, carrying out checks that only authorised software is in use and applying sanctions against unauthorised copying of software.

Use by the Wider Community

For school security and access reasons, at present there is no use of school equipment by the wider community.

Sanctions

This is the responsibility of the Headteacher.
All users – staff and pupils are subject to sanctions as outlined below if misuse of the systems is encountered.

Pupils: All Internet and ICT work is supervised at all times, therefore transgressions will be treated as would any unacceptable behaviour within the school. Sanctions will be as outlined in the school 'Behaviour Policy.' Computing forms part of the National Curriculum so it is unacceptable to 'ban' pupils from such activities.

Staff: Should staff breach the 'Acceptable Internet Use Policy' then the case will be referred to the Governors Disciplinary Committee.

APPENDICES

I Staff Confidentiality Agreement

II Information Security Training Programme

III Security Incidents and Malfunctions Procedure

IV E-mail Guidance for Staff

V Parental consent for use of digital pupil images

Appendix I Staff Confidentiality Agreement

GILLINGSTOOL PRIMARY SCHOOL

STAFF CONFIDENTIALITY AGREEMENT

Member of Staff: _____

Job Title: _____

Date of Appointment: _____

I understand that, as a result of employment at Gillingstool Primary School, I will be party to sensitive, restricted and confidential information, be it verbal, written or stored in electronic database form.

This information may concern pupils, parents or colleagues, and should be dealt with in a consistent and professional manner.

I agree to perform my job in a completely confidential manner at all times.

I understand that causing a breach of school confidentiality, or creating the circumstances that lead to breach of school confidentiality, may result in disciplinary action by the governors.

Signed: _____

Date: _____

Appendix II - Information Security Training Programme

GILLINGSTOOL PRIMARY SCHOOL

INFORMATION SECURITY TRAINING PROGRAMME

All new staff will:

- Discuss ICT Security with the Headteacher or Deputy Head on appointment. This will give the member of staff opportunity to clarify any issues before computer, Internet and e-mail access is granted;
- Be required to sign a 'Staff Confidentiality Agreement' – implications will be discussed;
- Have the 'Security and Malfunctions Incidents Procedure' outlined;
- Receive a copy of 'E-mail Guidance for Staff' if appropriate. This will be read in the presence of the Head and implications discussed;
- Read through the school's 'Acceptable Internet Use Policy', discuss the implications for pupils;
- Examine the 'Staff Internet Use Statement', discuss implications for themselves, and sign the statement;

Following agreement to the 'Staff Internet Use Statement':

- Appropriate passwords will be given;
- An e-mail account will be opened if appropriate (…..@southglos.gov.uk)
- Staff ICT capability and understanding will be discussed and assessed leading to the planning and provision of appropriate training.

Appendix III Security Incidents and Malfunctions Procedure

GILLINGSTOOL PRIMARY SCHOOL

SECURITY INCIDENTS AND MALFUNCTIONS PROCEDURE

Security and Filtering

Should any staff discover incidents of breaches of school ICT security then they should immediately inform either: Head Teacher
Deputy Head
School Business Manager

It is their responsibility to take appropriate action based upon established procedures, advice of
South Glos ICT Help Desk

Should staff accidentally discover any breaches of Internet and e-mail filtering systems, then they should record the matter in writing and immediately inform either:
Head Teacher
Deputy Head

Staff should **not** investigate the matter further as this may lead to further or greater breaches.

Staff should **not** seek to prove any system weaknesses, as this can be interpreted as a misuse of the system, potentially leading to disciplinary action.

Malfunction

Should staff experience any hardware or system malfunction then this should be reported to either:
Headteacher
School Business Manager

It is their responsibility to undertake recovery, or to refer the matter to the approved companies:
South Glos ICT Help Desk

Appendix IV E-mail Guidance For Staff

GILLINGSTOOL PRIMARY SCHOOL

E-MAIL GUIDANCE FOR STAFF

The e-mail facility is provided by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any use of e-mail.

All staff who use school ICT equipment will be required to sign the 'Acceptable Internet Use Policy' before an account and password is set-up.

- Access should only be made via the authorised account (….@gillingstool.org.uk) and personal password, which should not be made available to any other person. All school information and data must be sent via this secure email system and not via any other account;
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden and may lead to disciplinary action by the Governors;
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Posting anonymous messages and forwarding chain letters is forbidden;
- All e-mail activity should be appropriate to staff professional activity. Legitimate private interests may be followed where these cause no difficulties for other users and do not compromise school use;
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded or may be sent inadvertently to the wrong person. E-mail is not a secure medium;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden and may lead to disciplinary action by the Governors;
- Sending or displaying offensive messages or pictures, using obscene language, harassing, insulting or attacking others is forbidden and will lead to disciplinary action by the Governors.

(Should any member of staff breach the guidance as set out above, then disciplinary action may be taken)

Appendix V Parental consent for use of digital pupil images

GILLINGSTOOL PRIMARY SCHOOL

IMAGE / PHOTOGRAPH CONSENT FORM FOR SCHOOL

Image(s) required for…..	**School Website**
Council Contact	**Headteacher 01454 866527**
School and Photographer	**Gillingstool Primary School**
Date	**Photos taken from September 2017**

About the subject of the image(s) (Insert your child's name)	
Name	
Address	
Age	

The image(s) taken of the subject detailed above may be used for any publication by South Gloucestershire Council for:

Promotional, Information or Training purposes in print*****

Promotional, Information or Training purposes in moving images (video/film)*****

The school's website*****

*Please delete as appropriate

Please tick box I am the parent/guardian/carer of the subject of the image(s) ☐ (Required if the subject is less than 18 years old)	
Signed	
Print Name	
Date	

Please return to Gillingstool Primary School

Headteacher

Tel: 01454 866527

Fax: 01454 866528

E-mail: office@gillingstool.org.uk

Web site: www.gillingstool.org.uk

Gillingstool

Thornbury

Bristol

BS35 2EG

Date

Dear Parents/Carers,

We are continually adding more photographs of the children (e.g. school trips, Christmas performances, working in classrooms etc.) on our school website so that you can see your child 'in action'.

New regulations require that, for public documents e.g. our website and the school prospectus, we have individual consent rather than notification from you if you do not want your child to be photographed. Our policy of only using first names with photographs complies with the regulations.

On the reverse of this letter is the consent form that we are required to send home in order to obtain your permission for the use of your child's photograph on our website.

Please return this as soon as possible to enable us to conform to the South Gloucestershire guidelines. If you have any queries or questions, please do not hesitate to contact me.

Yours sincerely

Headteacher