Acceptable Use Policy

This Policy was reviewed:	**Aug 2020**
Signed Chair of Governors:	**Julia Anderson**
Signed Head Teacher:	**Michele Battersby**
Next Review Date:	**Sep 2021**

ST SILAS PRIMARY SCHOOL
ACCEPTABLE USE POLICY

ST SILAS PRIMARY SCHOOL
ACCEPTABLE USE POLICY

Table of Contents

ST SILAS PRIMARY SCHOOL
ACCEPTABLE USE POLICY

Loving God and each other,
we work together to be the best we can be.

1. Introduction

This policy outlines the secure and safe use of technology and technological equipment at St Silas Primary School and on the shared St Silas Primary School, Cidari Education, BWD network.

St Silas Primary School and Cidari Education are committed to protecting employees, partners and students from illegal or damaging actions by individuals, either knowingly or unknowingly. St Silas Primary School, Cidari Education and the Local Authority will take appropriate steps to protect IT equipment, resources and environments from threats, including but not limited to unauthorised access, computer viruses, violation of privacy and interruption to service.

1.1 Purpose

The purpose of this policy is to:

- Define the acceptable use of St Silas' Primary School IT resources and equipment.
- Ensure all use of the IT resources and equipment is legal, ethical, and consistent with the aims, values and objectives of St Silas' Primary School , Cidari Education and the BWD LA.
- Inform all users of their personal responsibilities when using the school and LA IT resources and equipment and environment.
- To protect the St Silas' Primary School, Cidari Education and BWD LA IT environment from all threats whether internal or external.
- To ensure that those who use school, MAT or LA IT resources, equipment and networks are aware of the requirements of IT Security and Acceptable Use.
- To ensure that users are aware of their roles and responsibilities in applying, enforcing and complying with IT Security and Acceptable Use.

1.2 Objectives

The objectives of this policy are:

- To ensure that equipment, data and staff are adequately protected on a cost-effective basis against any action that could adversely affect the school.
- To ensure that staff users are aware of and fully comply with all relevant legislation and guidance around IT security and safe and acceptable use of IT.
- To create and maintain within the school a level of awareness of the need for IT security to be an integral part of the day to day operation so that all staff understand the need for IT security and their own responsibilities in this respect.

1.3 Definitions

For the purposes of this document the terms 'IT' (or 'IT system') 'IT environment, 'IT data' and 'IT user' are defined as follows:

- 'IT' (or 'IT system') means any device for automatic storing and processing of data and includes server computer, personal computer (whether laptop, tablet, network attached to a domain), workstation, desktop publishing system, office information system, messaging system, video display, any other similar device and peripherals for these devices.
- IT environment means any virtual, cloud, online, networked or computer based resource or facility available through the school or LA.
- 'IT data' means any information stored and processed by IT and includes programs, text, pictures and sound; **see Appendices 4 and 5**
- 'IT user' applies to any MAT employee, member of school staff, pupil or other authorised person who uses the school's IT systems and/or data.

1.4 Scope

This policy applies to all users of St Silas Primary School, Cidari Education and Blackburn with Darwen LA IT environment and equipment, and must be adhered to at all times. It also sets expectations for the appropriate, legal and safe use of all equipment in school, including devices belonging to staff and pupils.

It also covers:

- All equipment that is owned or leased by St Silas Primary School, or Cidari Education.
- Guest devices authorised by St Silas Primary School or Cidari Education.
- All employees, contractors and temporary staff, outsource agents and other workers at St Silas Primary School, Cidari Education or BWD LA who are responsible for the administration and management of the St Silas Primary School IT equipment and resources.
- All those who use the St Silas Primary School IT services including staff, students and visitors.

1.5 Expectations

The appropriate Acceptable Usage Agreement (AUA) should be signed by all staff and pupils, and a parent or guardian of each pupil. A signed AUA form should be returned before a user is permitted access to IT equipment and services. Signed AUAs are stored safely in the School Office. All school staff have a responsibility to familiarise themselves with the relevant sections of this policy before using the St Silas Primary School, Cidari Education, or BWD LA IT equipment and environment. Each staff user must read, understand and sign to verify they have read and accepted this policy before using the IT equipment and environment. **See Appendix 1**.

Any user found to have breached the terms of this policy, may be subject to the St Silas Primary School/Cidari Education disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

2. Compliance with Policy

The IT environment is provided to support learning within the School, Cidari Education MAT and BWD LA education system. All those accessing the St Silas Primary School IT environment will comply with all current legislation in England, in addition to any requirements placed on them by this security policy. This includes compliance with legislation designed to protect personal information, legislation covering software and similar intellectual property licensed from third parties, and co-operation with Law Enforcement agencies. If in any doubt, the user should seek advice from St Silas Primary School Online Safety lead.

2.1 Compliance with Policy for all users

The primary use will be to support school educational and pastoral activities. Full compliance with the acceptable use agreements and policy standards is expected, including:

- Compliance with and adoption of the agreed password standards (**Appendix 2**)
- Adoption of safe practices to ensure the integrity of the IT environment, password security and data security.
- Compliance with the appropriate reporting mechanisms should they suspect an account has been compromised, IT security breached or safeguarding issues arise.

The IT resources and equipment are provided primarily for the purpose of conducting and supporting learning and teaching activities; however personal usage of school, LA or personal equipment is permitted as long as that does not:

- Take place during lesson time or otherwise interfere with the user's professional role.
- Incur a cost not previously authorised by the school
- Generate profit for the user
- Bring St Silas Primary School, Cidari Education or the Local Authority into disrepute.

All users should be aware that usage may be monitored and/or recorded; misuse of the IT equipment and environment may lead to disciplinary action. In such situations, the Headteacher and Cidari Education will be the arbiters of whether or not the use was reasonable in the circumstances.

2.2 Compliance with Policy for all school staff

In general, the acceptable use standard for school staff is the same as for students except:

- It is acceptable for a member of the school staff to access and use one of their pupils' accounts, in order to assist the pupil in using the IT resources and equipment.
- Members of the school staff should not use any other users IT Service user account login for work or personal matters.
- Members of school staff should not share their login details with other members of staff.

2.3 Compliance with Policy for temporary users

All temporary users will be required to:

- Sign the acceptable use agreement and agree to abide by the requirements set out in this policy.
- Sign the relevant Online Safety AUA and agree to abide by the Online Safety Policy.
- Not share their temporary details with any other person unless instructed/authorised to do so by the Senior Leadership Team (SLT) or technical staff.

2.4 Compliance with Policy for Operations Staff and Authority Staff

Technical support staff may have access to other users' information and files within the IT environment. This information will only be accessed for operational purposes. It must never be copied outside the IT environment. Inappropriate access to, or misuse of, personal information within the IT environment will be considered a disciplinary offence.

3 IT Security

A number of different groups have responsibility within St Silas Primary School for aspects of IT Security.

3.1 Board of Governors' Responsibilities

The Board of Governors has ultimate corporate responsibility for ensuring that the school complies with the legislative requirements relating to the use of IT systems and for disseminating policy on IT security and other IT related matters. In practice, the day-to-day responsibility for implementing these legislative requirements rests with the Headteacher.

3.2 Headteacher Responsibilities

The Headteacher is responsible for ensuring that the legislative requirements relating to the use of IT systems are met and that the school's AUP/IT Security Policy is adopted and maintained by the school. The Headteacher is also responsible for ensuring that any special IT security measures relating to the school's IT facilities are applied and documented as an integral part of the Policy.

The Headteacher, in accordance with the School's Financial Regulations, shall ensure that an inventory of all IT equipment (however financed) is maintained and all items accounted for at least annually.

In practice, the day to day functions may be delegated to the Cidari IT team (including DataSpire), who will keep an inventory of equipment within their remit.

The Headteacher is also responsible for ensuring that the requirements of GDPR (**Appendix 5**) are complied with fully by the school. This is represented by an on-going responsibility for ensuring that the:

- Registrations under the Data Protection Act are up-to-date and cover all uses being made of personal data.
- Registrations are observed with the school.
- School has a current Data Protection Policy, clearly defining how they assess and record levels of protection data.
- Data is subject to GDPR.

In addition, the Headteacher is responsible for ensuring that users of systems and data are familiar with the relevant aspects of the Policy that the appropriate controls are in place for staff to comply with the Policy. The Headteacher or Chair of Governors should ensure that details of any suspected or actual breach are recorded and made available to Internal Audit upon request. The Headteacher or Chair of Governors must advise Internal Audit of any suspected or actual breach of IT security pertaining to financial irregularity.

3.3 Internal Audit responsibilities

Cidari Education is responsible for checking periodically that the measures prescribed in each school's approved Computer Security Policy/AUP are complied with, and for investigating any suspected or actual breaches of IT security.

Specialist advice and information on IT security may be obtained from external providers e.g. SWGfL who will liaise with Internal Audit on such matters.

3.4 School Responsibilities

The Board of Governors and the Headteacher are ultimately responsible for all school responsibilities.

The school is responsible for:

- Ensuring appropriate arrangements are applied for the removal of any IT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- Giving adequate consideration to the physical security of rooms containing IT equipment (including associated cabling). As far as practicable, only authorised persons should be allowed access to the school's server or servers that provide access to data.
- Defining and documenting the requisite level of protection for data and documents according to the information classification system.
- Defining and documenting appropriate levels of access to the network and associated resources including the various Learning Platforms and MIS.
- Ensuring staff with higher levels of access sign any additional documentation as required e.g. technology agreements.
- Ensuring the ethical and safe disposal of decommissioned equipment.
- Ensuring the integrity of data, both during repair of faulty equipment and the disposal of assets.

3.5 User accounts

Access to the environment will be by individual user accounts for staff, who will be required to comply with minimum password standards and also by individual accounts for pupils except for Reception and Year 1 children. See **Appendix 2** for guidance on standards for passwords.

- Enabled user accounts are available only for current staff and pupils.
- The user account of anyone who is under investigation for inappropriate use of the system must be disabled promptly.
- 'Generic' or group usernames (i.e. accounts that could be used by more than one person) will only be created in special circumstances and must be agreed beforehand by the SLT, Online Safety Lead and Cidari IT and access restricted as appropriate.

Access to another user's data may be given in exceptional circumstances. Should this be required users should seek advice from the Headteacher.

3.6 Equipment siting

Reasonable care must be taken in the siting of computer screens, keyboards, printers or other similar devices. Whenever possible, and depending upon the sensitivity of the data, users should observe the following precautions:

- Devices should be positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the siting of devices on which confidential or sensitive information is processed or retrieved;
- Users should avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users;
- A 'clear desk policy' should be implemented, i.e. hard copies of sensitive data are not left unattended on desks.

The same rules apply to school equipment in use at a user's home or when accessing sensitive data using home equipment.

3.7 Adult user's responsibilities

All users will sign a user agreement at an appropriate level, before using the school's IT equipment.
All users of the school's IT systems and data must comply with the requirements of this Acceptable Use Policy, which are summarised in the Acceptable Use Agreement which is attached as **Appendix 1**. Pupils will sign an appropriate acceptable use agreement (Online Safety Charter) and should be guided by school staff towards respecting and conforming to the expectations of this policy.

All users are responsible for:

- The use of their unique logon details (usernames and passwords), email address where provided and for all content that is transmitted, received and stored by their user account. It is of utmost importance that the password and access to a users account remains protected at all times. **See guidance document in Appendix 2**.
- Reporting concerns over password security immediately.
- Users are responsible for notifying the Online Safety Lead of any suspected or actual breach of IT security. Where the level of breach requires it, the Headteacher should inform Cidari..
- Looking after all computer equipment, ensuring they leave PCs and peripherals in the condition in which they were found.
- Reporting any damage to equipment immediately to an appropriate staff member.
- Ensuring any mobile devices used in school are, when not in use, switched off fully, connected for charging and stored in a secure place.

- Ensuring pupils in their care are reminded regularly of expectations around appropriate use of IT equipment security and Online Safety.
- Returning portable equipment signed out to them for updates/maintenance when requested to do so.
- Endeavouring to protect St Silas Primary School equipment and the network against viruses, malware and other forms of software based attacks by virus checking portable/removable devices and following only reliable known links.
- Reporting any inappropriate use of IT services.
- Following the IT Asset Protocol when taking any school or Cidari Education equipment off the school's premises.
- Users should report any incidents, either perceived or real, to the Online Safety Lead, who will then be responsible for escalating relevant issues to the Headteacher, IT team, Cidari or other organisation as appropriate.

Users should not make any attempt to disable or reconfigure any IT security measures or software, including Anti-virus software or seek to bypass any monitoring, filtering or security measures that are in place.

Users are responsible for ensuring all data requiring backup is stored on the Google Drive and not saved on individual computers (unless it cannot be stored otherwise).

3.8 Staff user's additional responsibilities

Where users have access to sensitive data, they will receive training on data security before accessing data at an appropriate level on the managed service network**.**

Staff users are responsible for:

- Protecting access to their account, and for maintaining the appropriate confidentiality of their data.
- Ensuring privacy of pupil data
- Storing data appropriately

3.9 The IT Team (DataSpire)

At St Silas Primary School we insist that all technical support staff fully understands and complies with the requirements of GDPR and all legislation around the control and storage of data. The IT team has responsibility for:

- Ensuring all data held on the curriculum server is backed up and this process meets Government baseline security criteria.
- Bringing any security incidents, either perceived or actual, to the attention of the Headteacher.
- Management of the IT network, IT equipment, systems and data including controlling access to these assets under the instruction of the Headteacher.
- Integrity of data during both repairs of faulty and disposal of equipment.
- Measures to guard against unauthorised access to data, such as ensuring that all data is held in a secure location.
- Ensuring approved security patches and service packs are in place on all devices.
- Administering the practical aspects of IT protection and ensuring that various functions are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.
- Keeping the Admin Server up-to-date via any third party if necessary.

4 Online Communication and Use of the Web to Download/ Upload Information

4.1 Provision

Internet access

The provision of internet access is owned by the Council and all access is recorded and logged. This supports the performance of internal investigations and the management of systems as well as helping to ensure compliance in accordance with the Regulation of Investigatory Powers Act 2000.

Users browse the internet through a filtered service that is designed to reduce the risk of access to inappropriate material. Nevertheless this filtering cannot be 100% effective, and users should be aware of the possibility of access to inappropriate material and know what to do if such material is displayed (See the school's Online Safety Policy). Please note that this service is managed by BWD LA. Where a user's job role requires them to access sites that may be considered inappropriate approval must be obtained from their headteacher prior to access.

Staff with access to Cidari Education, BWD Schools, or BWD LA email should be aware that the content of emails and attachments may need to be disclosed under the Data Protection Act 1998 (**see Appendix 5)** and the Freedom of Information Act 2000. Email use is filtered and can be recorded.

The school, Cidari Education and the LA provide facilities for publication on the World-wide Web for school-related information, tools to communicate across the school community and tools to upload and publish ideas and resources.

Communication through the various other learning platforms may be permitted, but pupils will receive Online Safety education before using the system (for further information, please see the St Silas Primary School Online Safety Policy).

4.2 Guidance on use

All use of electronic forms of communication or use of the web to share, access downloads or publish information, should:

- Ensure that personal and financial information is safeguarded, including personal contact details.
- Ensure the security of the IT network by maintaining up to date virus protection and following links downloading files from reliable sources only.
- Always use a 'Cidari.co.uk, blackburn.sch.uk, or blackburn.gov.uk' email address when sending, receiving or forwarding emails containing RESTRICTED information.
- Access newsgroups, bulletin boards and other similar communication groups for educational purposes or those relating specifically to their professional role only.
- Use social networking sites, real time chat, discussion forums, online games and other similar web resources only when expressly permitted to do so for educational purposes, or as part of a member of staff's professional role.
- Only publish information after permission for use has been sought from the school and individuals
- Abide by copyright laws and licensing constraints regarding the use of software and electronic media.

Boundaries around publishing publicly accessible information and resources will be agreed by school SLT, with staff given appropriate permissions and clear guidelines as to acceptable content.

Use of electronic forms of communication or web access to share, download or publish information, for the following purposes is not permitted and may result in disciplinary and legal action where necessary. This includes but is not limited to;

- Sending, receiving, accessing or downloading obscene, racist, or insulting language, images, video or other media.
- Sending, receiving, accessing or downloading content in any form, containing provocative, suggestive or discriminatory language.
- Engaging in activities that bully, harass, mislead others or cause distress to groups or individuals.
- Accessing sites that are violent, hateful and discriminatory, promote hacking, or encourage gambling.
- Revealing information of a personal or private nature, or information that may lead to identification of an individual.
- Sending SPAM
- Downloading, uploading, sharing or copying any content of copyrighted material, unless permission has been sought and given by the owner of the copyright (please note breaching this is a criminal act and may lead to personal prosecution).
- Forwarding emails or information containing personal, confidential or sensitive information (therefore classified as PROTECTED or RESTRICTED information - **see Appendix 3** - from Cidari.co.uk, blackburn.sch.uk, blackburn.gov.uk email addresses to any personal email addresses including the employee's own personal email.
- Sending or forwarding emails containing RESTRICTED information to recipients outside the school who do not have 'Cidari.co.uk, blackburn.sch.uk, blackburn.gov.uk' email accounts (other authorised recipients of this information must receive emails that are encrypted).
- Using the St Silas Primary School/Cidari Education and LA IT Systems to support private business or money making activities.
- Any use that may potentially bring the users, the school and or the local authority into disrepute (where a user is unsure whether a particular use is acceptable, it is their responsibility to consult the Online Safety Lead, or Headteacher).

5 Mobile Devices and External Connections

Facilities are in place to allow the transfer of information into and out of the St Silas Primary School IT environment by removable media (e.g. pen drive, flash memory card, removable hard drive etc). Automatic antivirus and security tools are in operation to scan material during such transfers. All teaching staff have been issued with encrypted pen drives and all staff laptops are encrypted.

5.1 External Network Connections

Requests for external connections to access the LA IT Network, must be brought to the attention of BWD LA IT, who will establish whether it is safe to permit such access. This is the responsibility of Cidari Education IT.

5.2 Removable Media (pen/flash drives etc.) and Mobile Devices

Securing PROTECTED or RESTRICTED data is of paramount importance – particularly in relation to St Silas Primary School, Cidari Education and the LA. There is a need to protect data in line with the requirements of GDPR. When using mobile devices and removable media:

- Permission should be sought from the Headteacher and an assessment of risks, especially relating to information assurance, should be carried out before taking mobile devices out of the school site. **See Appendix 3**
- Users should sign to acknowledge receipt of loan devices.

Users should not engage in the following activities when using devices (laptops, tablets etc.) and removable media:

- Any action designed to circumvent anti-virus and IT security measures when connecting school equipment to private networks, or when accessing LA resources through private networks.
- Storage of PROTECT or RESTRICTED material. **See Appendix 4**
- Storing any data on removable media or mobile devices once it has been transferred/used.

5.3 Devices connected to the school, or Cidari Education IT network

Any device connected to the St Silas Primary School, Cidari Education, or LA IT network must comply with the following rules:

- All network servers and desktops must have adequate, up-to-date anti-virus protection or end-point security tools with automatic updates.
- Up-to-date security patches and service packs must be in place on all devices.
- Authority must be sought from the IT Manager before guest devices can be connected to the school network.

Any loss or theft of removable media or devices must be reported immediately to the SLT.

6 Storage and installation of Software, Resources and Data

The use and storing of information by the school, Cidari Education and LA is controlled by certain Acts of Parliament. There are obligations for the School and members of its community that must be followed. See Appendix 5

The owner has the legal title to the property. In this respect, all software, data and associated documentation produced in connection with the work of the school are the legal property of the Local Authority, which will normally hold it for the benefit of St Silas CE Primary School.

Exceptions to this will be allowed for software and documentation produced by individual teachers when agreed by the Online Safety Lead, Headteacher, or Cidari Education IT

We also use software and data that are the legal property of external organisations and which are acquired and used under contract or licence.

6.1 Licenses

Software license compliance requires all software used within the School is legally licensed, in accordance with the Copyright, Designs and Patents Act 1998.

It is the school's responsibility to ensure that all software (including) software on the IT network is appropriately licensed.
The school is responsible for compiling and maintaining an inventory of all software held by the School and for checking it at least annually to ensure that software licences accord with installations.

To ensure the School is compliant the following rules must be adhered to:

- All software must be purchased with a licence appropriate to its intended use.
- The school, Cidari Education and LA expressly prohibit the illegal duplication of software.
- Copying, downloading and storing of copyrighted material (such as music, and photographs from magazines) that is not waived for educational use is strictly prohibited.

- It is the school's responsibility to ensure that software added to all devices and desktops including guest devices, is appropriately licensed.

Please be aware that failure to follow this policy could lead to criminal prosecution.

6.2 Data Ownership

Data within the St Silas Primary School IT environment will be owned by a number of different individuals and organisations. Cidari Education will have the final decision on the ownership of any particular item. All data will be handled in a manner appropriate to its sensitivity.

6.3 Legal Responsibility

Cidari Education,Blackburn with Darwen Borough Council collects, holds and uses data about people and organisations with whom it deals with in order to conduct its business. They fully endorse and adhere to the Principles of Data Protection as set out under GDPR, and other relevant information security legislation. Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Key records must be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements**. See Appendix 5**

6.4 Protection of Data

The Authority and school will take appropriate steps to prevent loss, or incident, whether accidental or malicious, including error, fraud, damage and disruption to computing or communications facilities.

7 Dealing with incidents of unacceptable or inappropriate use.

7.1Systems and Security Monitoring

All users should be aware that in order to provide a secure environment the following detective security controls are in place:

- The Cidari email system is filtered and recorded (access to emails can be gained through the necessary channels)
- Web usage is actively filtered and recorded
- System usage may be recorded
- The school uses remote control and monitoring software to maintain network computers.
- System files, etc. may be accessed to ensure confidentiality integrity and availability.
- All users are responsible for the security of IT systems, including appropriate use of resources such as email and the internet.
- Parents and carers will be informed of the expectations and responsibilities of their child when using IT equipment and the school's learning platforms and encouraged to support their child in fulfilling the expectations.
- Any user data retained by filtering systems will not be released unless authorisation has been given by the Headteacher or an appointed member of staff (in line with GDPR).

7.2 Reporting

Any inappropriate or unacceptable use of the school/Cidari Education IT equipment, resources or personal devices during school time should be reported to the Headteacher or appropriate member of SLT.

All reporting procedures for the school should be in line with the legal requirements and other school policies e.g. child protection, data protection and disciplinary.

7.3 Consequences

St Silas' Primary School, Cidari Education, or local authority reserves the right to suspend or terminate an account if a security breach is encountered. The unacceptable use will be investigated as a security incident and the school or Cidari Education will decide on the appropriate disciplinary action.

Any violations of this security policy should initially be brought to the attention of the Online Safety Lead. Violation of this security policy by a member of school staff may lead to disciplinary proceedings and/or legal proceedings against that individual. Intentional or persistent violation of this security standard by staff of third parties in a contractual relationship with St Silas

Primary School, will be treated as a breach of the appropriate contract. Where a pupil is involved in intentional persistent violation of this policy, appropriate action will be taken by the Headteacher.

7.4 Incident Response Investigations

It is particularly important that all security and online safety incidents are logged and that a detailed record is kept of the investigation and resultant actions. All security incident reports and logs must remain confidential and only authorised personnel will be permitted to view this material. The investigation should, wherever possible, determine the extent of an incident, the impact of the incident, and the source of the incident. It may not always be possible to complete such investigations, but an attempt should be made to get far enough to make a reasonable recommendation as to actions that should be taken as a result of the incident.
Local law enforcement agencies will be contacted if the severity of a security breach necessitates this course of action.

Investigations are normally conducted for all security incidents including but not limited to the following:

- Unauthorised access or an attempt to access a resource or other users account without approval.
- Unauthorised modification to systems whether successful, or unsuccessful.
- Unauthorised disclosure of school information.
- Deliberate or unintentional hacking attempts.
- Rogue software, or hardware appearing on the St Silas Primary School/Cidari Education network.

8. Policy review

This policy will be reviewed by the school annually. Due to the rapidly changing nature of technology, this policy may be updated more regularly as a result of advice from the LA. Any changes should be shared with staff at the earliest possible opportunity.

Appendix 1

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's Acceptable Use Policy and Online Safety for further information and clarification.

- IT equipment and software are the property of the school/Cidari Education/Local Authority and I understand that it may be a criminal offence to use it for a purpose not permitted by its owner.
- I understand that I am responsible for my own use of technologies, and will ensure that I use technology safely, responsibly and legally.
- I understand that school and personal IT equipment may be used for private purposes out of school directed time only and that the use of school equipment may be monitored and should be in keeping with my professional status
- I understand that I must not use school IT resources for personal financial gain, gambling, political purposes or advertising.
- I understand that my information systems and internet use is subject to filtering and as such may be recorded.
- I will respect copyright and intellectual property rights. I will ensure that I have appropriate permissions before using or adapting work that may be the intellectual property of others and will acknowledge the source of all work that is not my own. **See appendix 5**
- I understand that it is my duty to protect my passwords and personal network login and should log off the network or lock the device before leaving it unattended.
- Never share including, but not limited to; uploading, posting , tweeting etc. any medium including, but not limited to; videos, pictures and text etc. that have negative connotations with reference to the school, its pupils, staff or directly contravenes legal statutes.
- I will seek advice prior to installing new software or hardware.
- I understand my personal responsibility for safeguarding and protection of data and will comply with the data protection Act of 1998 and any other legal, statutory or contractual obligations that the school and LA inform me are relevant. **See appendix 5**
- I will report any known misuses of technology, including the unacceptable behaviours of others to the Headteacher/appropriate member of SLT.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safeguarding to the designated senior person responsible for child protection.
- I will report any incidents of concern regarding suspected, or actual failure of technical safeguards to the school Online Safety Lead.
- I will ensure that any electronic communications with pupils are appropriate to my professional role.
- I will ensure that all electronic communications are written in a professional manner and understand that they are potentially public property.
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to use IT equipment and to the content they access or create.
- I understand that it is my duty to respect technical safeguards in place and will not attempt to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services.
- I will take reasonable precautions to prevent damage to or loss of IT equipment in my charge.

The school may exercise its right to record and monitor the use of the school's technology, including Internet access and email. The school will take the necessary action where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

- **I have read, understood and will abide by with the Information Systems Code of Conduct.**
- Signed: .... Capitals: .... Date: ....
- Accepted for school: .... Capitals: ....

Appendix 2

Password security guidance

- Staff should use a strong password and keep it confidential. Never write your password down or store it in a computer system. (A strong password contains a mixture of numbers, letters and punctuation)
- Never reveal your passwords to anyone (includes colleagues, BT&IT Service Desk, Line Managers, family and friends)
- Never use the 'remember password' function.
- All users must prevent their username and password being used to gain unauthorised access by locking the workstation when it is not in use so that casual overlooking and unauthorised tampering is prevented.
- If you become aware, or suspect, that your password has become known to someone else, you must change it immediately *****where this is possible***** and report your concern to *****Online Safety Lead, or Headteacher*****.
- Only use the user account to store data that is associated with the school.
- Users must not divulge their account passwords to others, must not permit others to use their accounts, and must not use accounts intended for the sole use of other individuals.
- Log off when leaving the room unattended. It is wise to save work before locking the workstation.
- Do not attempt to use your colleague’s credentials.

Pupils in Years 2 to 6 must access their accounts (school and online networks) using their personal logons and passwords. The strength of the passwords will be set by Cidari Education.

Appendix 3

IT Asset Protocol

Where any IT Asset (any school, Cidari Education, or LA IT equipment) is taken outside the site it must be checked out by the relevant person upon leaving the Site and checked in upon return.

Whilst any IT Asset is outside the Site:

- The person who checked it out shall be responsible for taking all reasonable precautions and care of it and for its safe return;
- It shall not be left unattended in any place or vehicle (whether locked or unlocked) other than the residence of the person who checked it out;
- During Core Hours ensure laptops & any other digital equipment is secured when rooms are empty for extended periods other than school break periods. Outside Core Hours, when not in use, teacher/administrator laptops must either be locked out of sight or taken home by the member of staff.
- It shall not be used where there is any material risk of damage from liquids, impact or otherwise;
- It shall not be lent or entrusted to any other person;
- Any alleged theft MUST be reported to the police and a crime reference number obtained and until the number is obtained it shall be deemed to be a loss rather than a theft.

In using any IT Asset:

- users shall not attempt to modify or circumvent any antivirus or other security software;
- users shall not save any data to the Asset that may cause damage or interference or instability to the Asset or any part of the Asset, including any firmware, operating system or other software;
- Users shall comply with the Acceptable Use Policy when accessing the any services, local, network or on the Internet.

The School shall ensure that any student or employee using IT equipment out of school is aware of this protocol.

The school and LA shall use reasonable endeavours to ensure that staff and students are informed of all further rules and procedures established from time to time by the LA to protect the security of IT Assets.

Where any IT Asset not on long term loan is taken outside the school it shall be checked out by the relevant person upon leaving the Site and checked in upon return using a system that is in line with school policies.

Users with devices on long term loan are responsible for returning the device to school on a regular basis or upon request, to ensure updates are installed and general maintenance can be carried out.

Appendix 4

Information Classification

Information classification is a means of standardising the way information is assessed, marked and handled according to how confidential it is. The national Protective Marking System to classify information and has been introduced throughout the public sector as the standard framework to allow the safe and appropriate sharing and protection of information. Please familiarise yourself with the following 3 levels of classification from the Protective Marking System, which are referred to throughout this Policy:

Unclassified
UNCLASSIFIED is the lowest level of classification and covers all information which can safely be shared or is already publicly available.
Information is UNCLASSIFIED if:

- It is intentionally publicly available
- Disclosure would not adversely affect any individuals, external organisations or the school e.g. School literature, the school website, press releases, all items of public record.

Protect
PROTECT is the first level of sensitive information. Information should be classified as PROTECT if "compromise of information would be likely to affect individuals in an adverse manner."
The PROTECT classification should be used where disclosure would:

- Be likely to affect an individual or a small number of individuals in an adverse manner
- Cause substantial distress to an individual
- Breach proper undertakings to maintain the confidence of information provided by third parties (for example, breach commercial confidence with a supplier to the school).
- Breach statutory restrictions on the disclosure of information e.g. documents/emails containing name, address, NI, DOB, commercial terms & conditions.
- Most of the sensitive information which the school handles will be at the PROTECT level of classification.

Restricted
RESTRICTED is a higher level of classification than PROTECT and is used where "compromise of information would be likely to affect the national interests in an adverse manner".
The RESTRICTED classification should be used where disclosure would:

- Put an individual at significant risk of harm or long-term distress
- Release personal information for 1000 or more individuals that is not in the public domain, even if the information is not likely to cause harm or distress (i.e. the release of a large amount of PROTECT classified data relating to individuals).
- Significantly undermine public confidence in the Council or other public body
- Cause widespread disruption to the work of the Cidari Education/Council or other local public sector organisation
- Significantly impact St Silas Primary School, Cidari Education or the LAs ability to discharge its duties under the Civil Contingencies Act

The RESTRICTED classification will apply to a small amount of data which the school handles, primarily relating to highly sensitive information on individual students and staff. E.g. documents/emails containing, name, address, NI, DOB, Salary, Pension, Benefit details, investigations, fraud etc.

Appendix 5

Data Protection and Other Relevant Legislation including GDPR

The Legislation

5.1 Background

5.1.1 The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of IT systems, which comprise principally of :-

Data Protection Acts 1984 & 1998;
Computer Misuse Act 1990;
Copyright, Designs and Patents Act 1988
General Data Protection Regulation 2018

5.1.2 It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.

5.1.3 The general requirements arising from these acts are described below.

5.2 Data Protection Acts 1984 & 1998

The Data Protection Act exists to regulate the use of computerised information about living individuals and gives rights to individuals about whom personal data is recorded (Data Subjects). They may obtain personal data held about themselves, should be told about the use of personal data and can expect it to be accurate. The act places obligations on those who record and use personal data (Data Users). They must follow sound and proper practices, known as the Data Protection principles.Principle 7 requires that security is in place during the collection, use and storage of personal data.
Any requests to view personal data must be in line with the Data Protection and Access to Information procedures.

5.2.1 To be able to meet the requirements of the Act, the Headteacher is required to compile a census of data giving details and usage of all relevant personal data held on computer within the school and file a registration with the Data Protection Registrar. It is important that amendments are submitted where the scope of the system extends to new areas of operation. The 1998 Act is consistent with the principles established in the 1984 Act, but extends the regulation to certain manual records as well as computerised information. This shows you how to log on to the Information Commissioners Site and pay the necessary £35.00 for registration.

5.2.2 It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.

5.2.3 Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Data Protection Registrar.

5.3 **Computer Misuse Act 1990**

5.3.1 Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:

- Unauthorised access to a computer system or data;
- Unauthorised access preparatory to another criminal action;
- Unauthorised modification of a computer system or data.

5.3.2 All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in-house', will be regarded as a breach of school policy and may be treated as gross misconduct and that in some circumstances such a breach may also be a criminal offence.

5.4 Copyright, Designs and Patents Act 1988

5.4.1 The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.

5.4.2 If an organisation is using illegal copies of software the organisation may face not only a civil suit, but corporate officers and individual employees may have criminal liability. If liability is proven this could lead to an unlimited fine and up to ten years imprisonment per offence.

5.4.3 Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.

5.4.4 All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.

5.4.5 All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

The Regulation of Investigatory Powers Act 2000

The Act specifies that communications may be monitored and recorded for "a legitimate purpose" such as system and employee performance monitoring; detection and prevention of crime; detection of unauthorised use (including unauthorised use by employees; protecting against hackers and viruses; and ensuring the Council is complying with regulatory or self-regulatory practices or procedures relevant to the business.

Monitoring can only be carried out legally if the organization concerned has informed its staff that it is undertaking monitoring for these purposes. The provisions of the RIP Act have been taking into account in the formulation of Council policy relating to email and telephone use as detailed later in this document. Consistent with the LA and St Silas CE Primary School policies.

General Data Protection Regulations 2018

The General Data Protection Regulation (GDPR) is the European Union's new regulation on data and cyber-security. It's designed to strengthen data protection for everyone, and that includes children and their families. GDPR are guidelines governing how organisations like schools handle personal data. The new regulations have replaced the current Data Protection Act (DPA) and were legally enforced from 25 May 2018.

Appendix 6

Unacceptable Use
This section does not provide a complete list of usage and behaviours that are considered unacceptable but it gives some examples of unacceptable use, in order to help all users of the IT Service to make decisions on unclear areas.

The following activities will always be considered unacceptable use of the St Silas Primary School IT environment by any user:

- Development, or deliberate release, of rogue code (i.e. viruses, ransomware etc.).
- Interference with the work of other users (e.g. altering or copying their work).
- Grooming, hacking, probing, scanning or testing the weaknesses of a system / systems within the St Silas Primary School/Cidari Education IT environment, or on the internet. Unauthorised access to systems. Violating or attempting to violate the security of the network.
- Actions that bring the school, Cidari Education, or the St Silas Primary School IT environment, into disrepute, or that are likely to do so.
- Deliberately wasting resources (e.g. unnecessary copying, or excessively copying for personal use).
- Use of the environment for personal financial gain.
- Any illegal activity, including breach of copyright.
- Attempting to log on using another person's username and password.
- Making your username and password known to any unauthorised person.
- Creating or storing offensive, intimidating, insulting or harassing material on the school network (virtual, or otherwise).
- Sharing including, but not limited to; uploading, posting , tweeting etc. any medium including, but not limited to; videos, pictures and text etc. that has negative connotations with reference to the school, its pupils, staff or directly contravenes legal statutes.
- Accessing data not intended for you to access.
- Attempting to bypass filtering, or to access inappropriate or illegal material – such attempts will be reported to the school authority.
- Leaving your workstation logged in while unattended.
- Connecting additional devices to data points on the IT network without the specific agreement of IT service provider.
- Attempting to interfere with services to any user, host or network.
- Taking any action in order to obtain services to which you are not entitled.
- Conducting any unlawful or illegal activity.
- Using the services to create, transmit, distribute or store content that invades the privacy or other personal rights of others.
- Assisting, encouraging or permitting any persons in engaging in any of the activities described in this section.
- Sending communications which result in complaints from the recipient or from the recipient's communication provider, or which result in blacklisting of the sender's email address or mail server.
- Sending email or messages which are excessive and/or intended to harass or annoy others.
- Sending, or attempting to send, spam of any kind from third-party networks using a return email address that is hosted on the IT mail servers, or referencing an email address hosted on the IT mail systems.
- Failing to observe intellectual property.
- Keeping, accessing or transmitting confidential data about other students or staff.
- Producing documents or emails that contain obscene, offensive, unlawful, intimidating, defamatory, harassing, abusive, fraudulent, or otherwise objectionable content as reasonably determined by the school or authority.
- Any use that interferes with, or prevents, another user's permitted use of the environment.
- Unauthorised modification or reconfiguration of St Silas Primary School/Cidari Education IT systems,
- Using managed service email or messaging systems to engage in inappropriate or non professional communications between either staff, staff and students or students.
- Any uses of school/Cidari Education IT equipment or personal equipment connected to the network, intended to bully or harass others.