SHERBORNE AREA SCHOOLS' TRUST

Staff ICT Acceptable Use Policy

Revised:	**01 June 2018**
Review due:	**June 2019**
Author:	**Network Manager**

SHERBORNE AREA SCHOOLS' TRUST
Staff ICT Acceptable Use Policy

1. Purpose

This Acceptable Use Policy is aimed at encouraging responsible behaviour and good practice. It has been created with the view to:

1.1 Ensure compliance and enforcement of relevant legislation which include but is not limited to the Computer Misuse Act and the General Data Protection Regulation;
1.2 Ensure the safety and integrity of students, staff and others;
1.3 Prevent damage to our schools and physical property.

2. Policy Statement

2.1 S.A.S.T. reserves the right to amend this Acceptable Use Policy, at any time, without notice. It is your responsibility to ensure that you are up to date with such changes.
2.2 This Acceptable Use Policy replaces and supersedes all previous versions.

3. Electronic mail (e-mail)

3.1 All members of staff, Trustees and Local Governors will be provided with email services for school related communication.
3.2 Caution should be exercised when sending confidential information via e-mail.
3.3 The transmission of confidential information via e-mail to unauthorised persons is strictly prohibited.
3.4 The use of e-mail for personal purposes is permitted but must be reasonable.
3.5 While S.A.S.T. respects the privacy of staff and volunteers, where there is reason for concern, the school reserves the right to monitor and intercept e-mail communication.
3.6 Any e-mail communication made must not bring S.A.S.T. into disrepute; this includes anything libellous, defamatory or criminal.

4. Internet Access

4.1 S.A.S.T. will only provide access to the Internet on receipt of a signed Acceptable Use Policy.
4.2 All Internet access is logged for the purposes of maintaining standards of security and acceptable use.
4.3 Attempts to access inappropriate websites or websites which attempt to bypass filtering systems constitute a breach of this Acceptable Use Policy.
4.4 Inappropriate websites referred to in **4.3** include, but are not limited to any site which contains:

- Pornographic Material (of either a legal or illegal nature);
- Material which incites hatred or discrimination;
- Material which promotes illegal activity;
- Material which is in breach of the Copyright Designs and Patents Act 1998;
- Material which is degrading to persons or groups of persons with particular characteristics;

4.5 Staff are required to report any website that they become aware of, which is not filtered, that is deemed inappropriate as per the criteria stated within **4.4**.

4.6 Staff should refrain from downloading large files during school hours as this may affect the quality of service for other users.

4.7 While S.A.S.T. , in conjunction with SWGfL, uses sophisticated filtering technology and takes all precautious to ensure that users only access appropriate material, it is not possible to guarantee that unsuitable material will be inaccessible. S.A.S.T. cannot accept liability for the material accessed, or any consequences of such access.

5. Network Access

5.1 Staff logins must only be used by the member of staff that they are issued to. Liability remains with the logged in user.

5.2 Allowing another person to use your login is a severe breach of this Acceptable Use Policy and contravenes legislation. Students must not use staff login under any circumstance.

5.3 Passwords must never be divulged to anyone at anytime.

5.4 If it is suspected that a password has been compromised it must be changed immediately.

5.5 Staff and volunteers will not attempt to download or install software onto the network or IT Equipment.

5.6 It is prohibited to copy any software or inappropriate material on to the network.

5.7 Staff and volunteers will not store confidential material on network areas which are accessible to persons who do not have clearance to access such material.

5.8 Staff and volunteers understand that the right is reserved to remotely monitor and intercept network activity.

6. Legislation

6.1 All network users are bound by current relevant legislation. The applicable laws (as amended) include, but are not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1998
- Criminal Justice Act 1988
- Defamation Acts 1952 and 1996
- Freedom of Information Act 2000
- Human Rights Act 1998
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1988
- Protection from Harassment Act 1997
- Public Order Act 1986
- Race Relations Amendment Act 2000
- Telecommunications Act 1984
- General Data Protection Regulations 1994 and 1998, 2016
- Sex Discrimination Act 1986
- Regulation of Investigatory Powers Act (RIPA) 2000

6.2 Staff and volunteers should understand that any attempt to bypass S.A.S.T. or other network security systems, including the introduction of viruses or applications of a destructive nature could lead to prosecution.

6.3 Where it is believed that a member of staff or volunteer in breach of legislation appropriate action will be taken.

7. ICT Equipment and Suites

7.1 Staff may not move or authorise any person to move any ICT Equipment.

7.2 Staff may not pass on any ICT Equipment to any other person. It must first be passed back to the ICT Support department and then reissued.

7.3 Any equipment issued to staff remains the property of S.A.S.T. and must be returned upon request.

7.4 Upon termination of employment at S.A.S.T. all equipment must be returned.

7.5 Staff are responsible for all equipment issued to them and must take reasonable precautions to protect such equipment, including complying with insurance requirements of securing equipment at all times.

7.6 Staff are responsible for all equipment and use of workstations by students during their lessons in ICT Suites. Their department will be billed for any associated damage.

7.7 Staff must ensure that ICT Suites are locked upon leaving the room. Students should not be allowed access to keys to ICT Suites at any time.

7.8 Staff should report unlocked ICT Suites.

7.9 No students may be allowed to use ICT Suites without suitable supervision by a member of staff. (This does not apply to sixth form students using IT5)

8. Personal Use of ICT Equipment

8.1 The computers and other ICT equipment provided by S.A.S.T. are primarily for business use to assist staff in the performance of their jobs. Limited, occasional or incidental use of this equipment for personal, non-business purposes is understandable and acceptable and all such use should be undertaken in a manner that does not negatively affect the equipment's use for business purposes. However, staff are expected to demonstrate a sense of responsibility and not abuse this privilege**.**

9. Additional Systems

9.1 Members of staff may have access to additional systems which include, but are not limited to: e-portal or facility admin.

9.2 These systems require additional passwords. It is the responsibility of the member of staff to ensure that their password has basic complexity to it and that their password is only known by them.

1. Sanctions

In the event that this Acceptable Use Policy is breached, staff will be subject to sanctions which may include, but are not limited to:

- Disciplinary procedures;
- Temporary or permanent restriction of network access;
- Temporary or permanent revocation of network rights;
- Restriction to or denial of access to ICT Suites;
- Investigation under the Regulation of Investigatory Powers Act (RIPA) 2000.

Key Point Summary

The staff acceptable use policy has been modernized in order to keep up to date with the new technologies that are being used. A copy will be e-mailed to all staff at the beginning of the academic year.

The aim of the policy is to protect both staff and students when using ICT equipment. The document covers:

1. E mail usage
2. Internet Usage
3. Network Access
4. Key Legislation
5. ICT Equipment and Suites
6. Personal Use of ICT equipment
7. Additional Systems
8. Sanctions

With increased student data being held on the system and the increased internet access for staff which we hope to achieve it is important that we as users are responsible in our usage. This includes:

- Reporting any incidents which occur to the ICT team so that they can be dealt with centrally.
- Not letting students use staff user accounts.
- Not leaving students to work unsupervised on machines which are hard wired into the school network.
- Locking the machine you are using if you need to leave the room temporarily.
- Being aware that the majority of software needs a licence to run in school and unlicensed software should not be used.
- Respecting bans that students may have been given for previous misuse.

If you have any concerns regarding computer usage please talk to Neil Burroughs (SAST Head of IT Services).

Staff Agreement

I have read and understood the Staff ICT Acceptable Use Policy for SAST.

I understand that should I be found in breach of the Acceptable Use Policy I may be liable to disciplinary procedures and, if appropriate, the Police and local authorities may become involved.

Staff Name *

*** USE BLOCK CAPITALS**

Staff Signature **Date** DD MM YY