The Good Shepherd Multi Academy Trust

Staff Acceptable Use Policy

February 2016

The Good Shepherd
Multi Academy Trust

Review February 2017

Values

Every member of the Trust family of schools will be valued and encouraged to fulfil their potential. In our Trust we believe:

- Everyone has something to offer
- Trust, honesty, empathy and social responsibility are the Christian values that frame our work
- We are here for the whole person, spiritually, morally, educationally and socially
- In working with transparency and openness

1. Scope

The Good Shepherd Multi Academy Trust's (the Trust's) networked resources, are intended for educational purposes, and may only be used for legal activities consistent with the rules of the Trust. If you make a comment about the Trust or any school or college within the Trust you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the Trust or any school within the Trust into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

2. Conditions of Use

2.1 Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to a member of the senior leadership team.

2.2 Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the Trust or any school or college within the Trust into disrepute.
2	I will use appropriate language –I will remember that I am a representative of the Trust on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4	I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

5	Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.
6	I will not trespass into other users' files or folders. Staff Accessing students work must be given permission before this can take place
7	I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual other than myself. Likewise, I will not share those of other users.
8	I will ensure that if I think someone has learned my password then I will change it immediately and/or contact a member of the senior leadership team.
9	I will ensure that I log off after my network session has finished, or will lock the computer to make it secure until my return.
10	If I find an unattended machine logged on under another user's username I will not continuing using the machine – I will log it off immediately.
11	I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the senior leadership team.
12	I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted. I am aware that all emails are backed up and that my emails in the backup may be searched if an investigation is required with or without my knowledge. I understand that my email account and other online/offline storage files can be searched if an investigation is required with or without my knowledge.
13	I will not use the network in any way that would disrupt use of the network by others.
14	I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to a member of the senior leadership team.
15	I will not use "USB drives", portable hard-drives, "compact disks" or personal laptops or any other device on the network (wired or wireless) without having them "approved" by a member of the senior leadership team or the school's IT provider.
16	I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use. I understand that all websites I visit are recorded and may be searched, with or without my knowledge, if an investigation is required.
17	I will not download/install any software, system utilities or resources from the Internet or digital device.
18	I will set up a secure pin code on my phone or similar connected device that is connected to the email system. I will also notify the Trust and the schools IT provider immediately if a phone or similar connected device which is connected to the email system is lost or stolen. This will give the opportunity to disable your email access from such device
19	I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role in any way.
20	I will support and promote the Trust or any school within the Trust e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.

21	I will not send or publish material that violates the Data Protection Act or breaching the security this act requires for personal data, including data held on the SIMS / iScholaris / Google Apps / Office 365 and SharePoint.
22	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
23	I will not attempt to harm or destroy any equipment or data of another user or network connected to the Trust.
24	I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.
25	I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.
26	I will not plug non-school equipment into an electric socket at the Trust office or any school within the Trust unless it has been PAT tested at school.
27	If I transport equipment between home and any Trust site or another destination I must not leave the equipment unattended.
28	I understand that my network activity can be logged and might be searched, with or without my knowledge, if an investigation is required. Permission to do so will only be instructed by the Chief Executive Officer.
29	I understand that I must follow agreed protocols when using an ICT room or any ICT resources within the Trust or any school within the Trust.
30	At any time and without prior notice, Trust management reserves the right to examine e-mail, personal file directories, and other information stored on the Trust or schools networks and equipment. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of Trust information systems. Permission to examine such information will only be granted by the Chief Executive Officer.

3. Additional guidelines

Staff must comply with the acceptable use policy of any other networks that they access. This includes any external system that the Trust or any school within the Trust is partnered with

3.1 Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The Trust or any school or college within the Trust will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

3.2 Network Security

Users are expected to inform a member of the senior leadership team or the school's IT provider immediately if a security problem is identified and should not demonstrate this problem to other users. Users identified as a security risk will be denied access to the network. Users who want to have their smartphone or internet connected device used for remote access or email should first be authorised to have this feature enabled by a member of the School Leadership Team and IT provider. Any connected smartphone or tablet must have a secure pin number set in order to

protect the email / remote access. Lost / Stolen devices should be immediately reported to the Trust IT Manager or a member of the Senior Leadership Team.

3.3 Media Publications

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.

Social Media and Messaging All users should be aware of the risks associated through using Social Media and Messaging in their professional role. Becoming friends or following students on social media platforms is not acceptable with the only exception being where a member of staff has children within a school in the Trust. Any use of personal social media that brings the Trust or any school within the Trust into disrepute will result in disciplinary action. Users should not use any form of internet messaging services within their role apart from those that are approved by the Trust.

Staff User Agreement Form for the Staff Acceptable Use Policy

As a user of The Good Shepherd Multi Academy Trust's network resources, I agree to follow the rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the Trust acceptable use policy. If I am in any doubt I will consult the headteacher in the first instance.

I agree to report any misuse of the network to the headteacher or the Trust.

I also agree to report any websites that are available on the school internet that contain inappropriate material to the headteacher.

Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to the senior leadership team.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: _____

Staff Signature (if appropriate): _____

Date: _ _ /_ _ /_ _ _ _