National Star
Realising the aspirations of people with disabilities

Version: 1.0
Creation Date: 01/03/2016
Creator: David Dalby

Acceptable Use Agreement: Staff

This agreement is to ensure that you use IT systems, IT equipment and online activity safely and responsibly in your work at National Star and that you are aware of accountability for all activities.

Associated polices and documents include eSafety; Email and Internet; Safeguarding including Prevent Strategy; Health and Safety; Social Media; Guidance for Safer Working Practice at National Star.

The term confidential means any information that could identify a student or member of staff, or is of a personal nature, including unauthorised use of media such as photographs and video.

Account Details
Do not share your account details with anyone else, and you must not log in as or use another member of staff's account. (IT Systems Team may require your password and may at times need to log in as another user for issue resolution). If you believe someone else knows your password inform IT Systems immediately.

Some learners and residents require support to log on, you may have access to their account details and log on for them. You should not give this information to others or use a learner's account on behalf of yourself

Take precautions to protect your personal accounts such as Facebook and Twitter to avoid unauthorised use. Change passwords if you believe the account has been compromised.

Equipment
All National Star equipment is predominately for business use. This includes printers, computers, laptops, phones and tablets.

All equipment remains the property of National Star and portable equipment such as laptops, phones or tablets issued are to be returned at end of contract or at the request of your Line Manager. You may be asked to return equipment during extended absence or change of role that does not require this equipment.

It is your responsibility to look after equipment and prevent damage or loss. This includes not leaving equipment on display in vehicles, in unlocked areas where the equipment could be removed or on display where it could encourage theft. Mobile equipment such as laptops and tablets may be used anywhere provided reasonable precautions are taken. Damage, loss or theft of any equipment due to negligence may be charged for

Ensure sensitive or confidential electronic information is not kept locally or on unencrypted removable media (eg memory sticks). If you require advice on encrypting removable media please contact IT Systems Department.

All media relating to National Star, <u>including all images and videos</u> should only be taken with and stored on National Star equipment.

Do not leave equipment logged on unattended at college or elsewhere at any time.

Any loss of equipment, including **your own** equipment such as phones or tablets that potentially contains confidential information (eg National Star email account on your personal phone) through loss or theft must be reported to the IT Systems Team immediately.

Data and Information

Personal data must be stored and used according to the Data Protection Act 1998 and National Star Policies and Procedures. Anything stored on a National Star system or equipment, including email, phone, files, laptops and tablets is owned by National Star. This may be accessed by a member of the IT Systems Team or Senior Member of the Human Resources with authorisation from a Senior Manager or Senior Member of the Human Resources Team without warning or your permission for any investigation.

On leaving employment with National Star all data including email and files continues to be owned by National Star. This may be made available for business purposes to other staff on authorisation by a Senior Manager. Organisational and business information must not be taken with you on leaving including student or staff details and photographs.

Transferring confidential information such as Student Care and Health Plans, medical information and Progress Reports must be done via a secure file transfer. Please refer to IT Systems Team if you require advice on this.

You should only store work related data on National Star equipment and systems. IT Systems are not responsible for data loss of any personal files and are unable to provide advice or repairs to personal equipment for students or staff.

Other people may have access to confidential documents saved to a shared space (eg Staff Shared Folder or the Intranet). If you are unsure who else has access you need to check with the departmental owner or IT Systems.

Portable devices such as phones, tablets and laptops whether National Star **or your own** that contains confidential information, including work email, must be encrypted and secured with a pin code as a minimum. Refer to the Bring Your Own Device statement available on the Intranet for more information. All removable media such as pen drives containing confidential information must be encrypted. If you require advice on encrypting removable media please contact IT Systems Department

Any potential loss of data through accident or theft must be reported to the IT Systems Team immediately. This includes any suspected unauthorised access to National Star systems.

Equipment must not be used to breach Copyright regulations or intellectual property rights.

Communications and Social Media

You are a representative of National Star and must not damage the reputation or bring the organisation into disrepute in any way. This includes not using inappropriate, threatening or offensive language.

All work related communications must use National Star accounts, including emails, video conferencing and secure file transfer. Use of Social Media through personal or National Star accounts must comply with the Social Media Policy.

Staff should not use personal accounts for email or Social Media with current students and be circumspect in their communications with former students so as to avoid any possible misinterpretation.

All activity on IT Systems is logged including internet history, email, printing and telephone use. This may be accessed by a member of the IT Systems Team with authorisation from a Senior Manager or Senior Member of the Human Resources Team without warning or your permission for any investigation.

Use of IT Systems and the Internet
Email, Intranet, databases and some other services are available for external use on any device. Ensure others cannot access your account by not saving password locally or using where others may be able to view.

You must not make attempts to breach network security settings. If you find you have access to an area you should not this must be reported to the IT Systems Team immediately.

The internet must not be used to access illegal or inappropriate information. Inappropriate includes pornography, hate, racist, sexist, or other offensive material. Robust filtering is in place and you should not attempt to bypass this. Equipment and systems must not be used for any illegal purposes, including illegal peer to peer file sharing sites.

Unless you have been given administration rights, if you require additional software or services that are not installed as standard or are no longer required and should be removed, submit as a support request to IT Systems.

Protect other's email addresses when sending externally by using Blind Carbon Copy (BCC). If you require advice on how to do this please contact IT Systems.

Avoid sending large files as attachments to multiple recipients.

Use email groups logically to keep communications to only necessary recipients. You should not email All National Star Staff and/or Students/Residents unless absolutely necessary.

Avoid emailing large groups of recipients externally as this could be seen as spamming. Split into less than 50 recipients or ask IT Systems for advice.

Departments are responsible for ensuring departmental specific software complies with licencing agreements.

Non-compliance with this agreement may result in your account being suspended and disciplinary action being taken.

If you require clarification of this agreement please contact your Line Manager.

Updates to this agreement will be issued by requesting a reacceptance.

Legislation, Regulation and other information relating to this agreement include:
Computer Misuse Act 1990
Telecommunications Act 1984
Copyright, Designs and Patents Act 1988
Regulation of Investigatory Powers Act (RIPA) 2000
The Data Protection Act 1998
Keeping Children Safe in Education 2015
The Children Act 1989 and 2004
The Protection of Children Act 1999
Working Together to Safeguard Children (Department for Education 2015)
Safeguarding Vulnerable Groups Act 2006

By signing you accept this agreement

Name:

Signature:

Date:

Please return to IT Systems Department