NS POLICY	IT and Social Media Acceptable Use Policy (AUP)
Senior Manager Responsible	Director of Technology Innovation
Policy Date	June 2017
Policy Review Date	June 2020
Superseded Documents	- Staff Acceptable Use Agreement from February 2016 - Email and Internet Policy - Social Media policy - E Safety Policy - Bring Your Own Device Statement - Internet & Email Code of Practice for Staff & Volunteers
Associated Documents	- Data Protection Policy - Disciplinary Policies - Anti-Bullying Policy - Safeguarding Policy - E-Safety *Flowchart* - Appendix A: Staff Acceptable Use Policy Declaration - Appendix B: E-Safety Flowchart - Appendix C – Rules for the use of social media

Impact Assessment		
Name – David Dalby	**Comments -** Policy written by IT Services with Director as an updates to previous versions to meet current legislation and combine 6 separate documents. Senior Management have reviewed the document agreed is presented to Board for agreement. Users had agreed to previous Version and will need to agree to new version.	**Date 8th October 2017**

Authorisation	**Authorisation Date**
Paul Styles	6th November 2017

History	**Name**	**Comments**
November 2017	P Styles	Board approval
June 2017	D Finch	New Policy

1. INTRODUCTION

1.1 Background and legal Framework

1.1.1 This policy has been created to update and replace the policies listed in the 'superseded documents' section. This policy brings together all IT related staff policies into one document. Note that in addition to this policy a set appendices are included at the end of the document.

1.1.2 For the purposes of discharging the organisations responsibilities under the Prevent Duty and to maintain the highest standard of safeguarding, this policy is directly linked to the Safeguarding policy as shown in Appendix B (e-Safety Flowchart). This Acceptable Use Policy (AUP) has been written using current advice from JISC (Joint Information Systems Committee).

1.1.3 We recognise the enormous benefits to be derived from the use of IT for both staff and service users; however there are risks that must be mitigated against. National Star will ensure staff and service users understand their responsibilities regarding e-safety in line with this policy through continuous training.

1.1.4 National Star aims to educate staff and service users about e-safety but this must be a collaborative effort to enable an organisation wide effective response. Using IT and the Internet is part of the organisations learning delivery and is integrated into many subjects and contexts.

1.1.5 This policy will enable all staff and service users to understand the acceptable and appropriate use of information technology. Staff using the organisations IT services must read and comply with this policy. All users must accept a declaration (appendix A) before using IT Services. This is an important undertaking as misuse of National Star's IT services could lead to disciplinary action; this could range from the loss of internet access to dismissal for gross misconduct. If this policy is breached it will be the staff member as well as the organisation that is held accountable for any resulting legal action. An example could be copyright violation – the downloading of copyright infringing films, software or music being possible breaches of the policy.

1.1.6 National Star operates various technological systems to assist in the maintenance of this policy; this includes monitoring and filtering systems. Such technological systems are not a complete solution and will only be effective when combined with an organisation wide commitment to the policy.

1.1.7 Through this policy, National Star aims to protect staff, and service users with particular reference to the following legislation:

Human Rights Act 1998
Computer Misuse Act 1990
Telecommunications Act 1984
Telecommunications (Lawful Business Practice, Interception of Communications) Regulations 2000
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
Obscene Publications Act 1959
Criminal Justice Act 1988
Working Together to Safeguard Children (Department for Education 2015)

Safeguarding Vulnerable Groups Act 2006
The Prevent Duty 2015

1.2 Purpose

The purpose of this policy is to;

1.2.1 Ensure staff use IT equipment and systems in a safe, legal and responsible way in order to discharge their duties.

1.2.2 Describe what is defined as acceptable use, including the use of IT services such as the Internet, email, e-safety and social media.

1.2.3 Clarify the responsibilities and accountabilities placed on users in their use of IT systems and equipment.

1.2.4 Ensure all users of IT services including staff and service users are protected from inappropriate material as well as ensuring that safeguarding procedures are applied when using IT services including the application of the Prevent Duty.

1.2.5 Ensure that National Star is compliant with current legislation, regulations and guidance as advised from JISC (Joint Information Systems Committee)

1.2.6 Ensure data availability and data integrity.

1.2.7 Outline the standards that National Star requires staff to observe when using social media, the circumstances in which the use of social media will be monitored and the action the organisation will take in respect of breaches of the policy.

1.2.8 Help staff make appropriate decisions about the use of social media such as blogs, wikis, social networking websites, podcasts, forums, message boards, and when making comments using Twitter, Facebook, Linked-In or other similar social media instruments.

1.2.9 This policy does not form part of any contract of employment and it may be amended at any time.

2. SCOPE

2.1.1 This policy covers all staff and service users working at all levels and grades, including senior managers, officers, directors, employees, trainees, apprentices, casual and agency staff and volunteers, governors and trustees (collectively referred to as staff in this policy).

2.1.2 This Policy applies to staff and applies when using National Star's IT services within and outside of the organisations sites. It applies when using either National Star equipment or personal equipment when accessing National Star data, services or representing National Star e.g. through social media.

2.1.3 All staff are expected to comply with this policy at all times to protect the interests of National Star and the individuals using the services, other employees and partner organisations.

2.1.4 Breaches of this policy may result in IT access being suspended and may lead to disciplinary action. Serious cases may be treated as gross misconduct, which may result in summary dismissal.

3. POLICY STATEMENT

3.1 User Accounts

3.1.1 Users of all IT services will be allocated an individual user account with defined access rights.

3.1.2 Users will be required to agree the terms of acceptable use before being able to access IT systems. Prior to being issued, these new accounts will be stored in sealed envelope in a secure cupboard.

3.1.3 Users are responsible for the security of their account and must not allow others to access the systems using their log on details (including, colleagues and/or family members). Users must immediately report any suspicion or breach of security. There may be exceptions where staff require access to an account that is not their own;

Some service users require support to log on and staff may have access to their account details in order to do this for them. In this instance these details will be stored in DataBridge with only the authorised staff having access. Staff must not share this information with others or use a service user's account for themselves. If a service user can remember their own password it is not necessary for staff to have access to their password.

IT Services Team may need to log on as a different user for issue resolution. In this event, the user will be notified beforehand and forced to change their password immediately after the issue is resolved.

3.1.4 Any misconduct detected on a user's account is deemed to be the responsibility of the user. If a user believes their password has been compromised, they must change it and inform IT Services immediately.

3.1.5 Users must take precautions to protect personal accounts such as Email, Facebook and Twitter to avoid unauthorised use. Change passwords if you believe the account has been compromised. We advise, you do not share personal account details as you remain responsible for actions performed under these accounts.

3.1.6 Users must not attempt or conceal attempts to use any IT service or equipment to access unethical, illegal or offensive material (including pirated music, movies and copyrighted material).

3.1.7 Users (staff only) must choose passwords that:

- Avoid obvious passwords (such as those based on easily-discoverable information like the name of a favourite pet);
- Avoid common passwords — this could be implemented by technical means, using a password blacklist;
- Are not used anywhere else, at work or at home.
- Is at least 15 characters or longer – (use pass phrases with spaces or four short words)

3.2 Equipment

3.2.1 All National Star equipment is provided for business and educational use. This includes printers, computers, laptops, phones and tablets. Equipment is only to be used by staff and service users.

3.2.2 All equipment remains the property of National Star and equipment issued to a user such as laptops, phones or tablets are to be returned at end of contract or at the request of the user's manager. Users may be asked to return equipment during extended absence or if a change of role no longer requires the use of such equipment.

3.2.3 It is the responsibility of the user to look after equipment with care and to prevent damage or loss. Users are encouraged not to leave equipment on display in vehicles or in unlocked areas. Damage, loss or theft of equipment due to negligence may incur repair or replacement charges by the user.

3.2.4 Any loss or theft of equipment, including personal equipment such as phones or tablets that potentially contain confidential information such as, National Star email account on your personal phone, must be reported to the users line manager and IT Services team immediately.

3.2.5 Only National Star equipment or equipment authorised by the IT Services team can be connected to one of National Star's networks. Guest wireless access can be provided by the Customer Services Team for Ullenwood or designated staff at other National Star sites. The guest network allows access to Internet resources and not National Star's internal network. Guest devices must never be connected to network sockets without authorisation by the IT Services team.

3.3 Personal equipment

It is the user's responsibility to ensure that any device used for National Star activities (including accessing National Star email or other services) comply with the following:

3.3.1 No photographs/videos (of either service users or staff) must be taken on personal devices

3.3.2 Ensure a locking passcode is used on any mobile device that is used for work email or other work related business

3.3.3 The device must be encrypted

3.3.4 The device must be running a supported operating system and be kept fully up to date with security updates

3.3.5 Ensure device tracking is enabled on devices (such as 'find my iPhone')

3.3.6 Maintain technical support of personally owned devices (whilst IT Services may be able to provide guidance, ongoing technical responsibility for personal devices resides with the user)

3.3.7 Lost devices containing any form of National Star data (this includes emails), must be reported to line managers and IT Services immediately.

3.3.8 National Star reserves the right to take further action (e.g. deletion of email account, locking or wiping of a device) in the event of a lost or stolen device

3.3.9 Not reporting a lost device containing National Star data such as an email account may be deemed a disciplinary offence and appropriate action may be taken

3.4 Security

3.4.1 National Star uses a range of anti-virus, firewalls and other protective hardware and software which are regularly maintained and updated to try and prevent accidental or malicious attempts that might threaten the security of the organisations IT services and data. The IT security systems are reviewed by senior members of the IT Services Team under the oversight of the Strategic Leadership Team and the audit committee.

3.4.2 Users must log off or sign out of any National Star IT service or equipment prior to leaving it unattended to prevent unauthorised access to data.

3.4.3 Users must not make attempts to breach security systems, mask their activity, circumvent web filtering, hack IT services, gain access to systems to which they are unauthorised to access or engage in any activity that could harm systems or data. Security violations or breaches in security measures (e.g. trying to bypass web filtering) must be reported to the IT Services Team.

3.5 Monitoring

3.5.1 Random checks of data on the system will be undertaken by IT services to both check that inappropriate material is not being stored and to control excessive use of storage.

3.5.2 Monitoring systems are continually logging activity (including; internet activity, emails, printing, phone calls) of all users and are retained for the purposes of technical troubleshooting and investigation (inclusive of safeguarding and Prevent Duty related concerns). Where these logs contain 'personal data' as defined in the data protection act (such as the web monitoring systems), access is strictly controlled. The web monitoring systems can be accessed by the senior IT Services staff, Head of HR and the safeguarding team in order to maintain this policy. Real time, automated alerts are generated when the monitoring policies are breached (e.g. excessive Internet use or trying to access blocked content). These alerts are sent to the safeguarding team, Head of HR and Head of IT Services for investigation. Targeted staff monitoring, if not triggered by an automated alert (as outlined above) will require authorisation by the Head of HR or Director as part of any investigation into potential misuse. Targeted service user monitoring will be authorised by the PLC (Personal Learning Coordinator) or respective provision manager.

3.5.3 Routine monitoring of summary logs will be undertaken to highlight any potential misuse and could trigger a targeted monitoring on Staff or service users. If the content is related to pornography, or hate or radicalising materials commensurate with the definition in the Prevent Duty, (or other inappropriate material) it will be treated as a safeguarding incident.

3.5.4 To support the organisation's response to the Prevent Duty, safeguarding or other police investigations, National Star may share requested information with the Police or other regulatory authorities. This could include copies of the logs of visited websites (by any user) or logs from other IT services.

3.6 Filtering

3.6.1 National Star provides enhanced user-level filtering. This is designed to prevent users accessing inappropriate websites including; extremist, illegal or obscene websites and resources. Amongst other things, this system allows National Star to determine who has accessed what material, from which computer, when, and for how long. This information can be used for investigations or to alert managers to potential issues.

3.6.2 Requests for sites to be removed from the filtered list fall into two categories. Firstly, incorrect categorisation by the filtering system, in this instance the IT Services Team will correct the error. Secondly, requests to change the filtering policy, in this instance the Safeguarding Officer will undertake a risk assessment, if approved the IT Services Team will unblock the website requested.

3.7 Accessing Services Remotely and Support

3.7.1 Remote management tools are used by the IT Services Team and authorised third party support providers to control workstations and view the screens remotely. These tools can only be used with the user's agreement or by the user running the tool to start the remote session. It's the users' responsibility to ensure nothing confidential is on the screen prior to allowing access. If the person providing support is not from IT Services, the user must receive authorisation from IT services and supervise any third party access while support is given.

3.7.2 Some IT services are available for external use on any device including: Email, Intranet and DataBridge. Users must only use these services when they can ensure others are not able to view the information. Users must not save passwords for these services on personal devices.

3.8 Software

3.8.1 The organisation prohibits users downloading or attempting to run/install executable files. Including, the installation of software onto our equipment. If additional software or changes are required users must log an IT Service request.

3.8.2 Departments are responsible for ensuring that departmental specific software complies with licensing agreements and copies of certificates and software must be provided to IT Services.

3.9 Data and Information

3.9.1 Personal and confidential data must be stored, proceeded, transferred and made available according to the Data Protection Act 1998 and organisation policies and procedures. The term confidential means any information that could directly or indirectly identify a service user or member of staff, or is of a personal nature, including use of media such as photographs and video.

3.9.2 Staff holding confidential information about the organisation and our service users must not make any of this information available to others without appropriate authorisation in accordance with the Data Protection Policy.

3.9.3 Anything stored on a National Star system or equipment, including email, phone, files, laptops and tablets is owned by National Star. If part of an investigation information held on the device may be accessed without prior warning or permission by a member of the IT Services Team or Managers with authorisation from a Senior Manager or Senior Member of the Human Resources Team.

3.9.4 On leaving employment with National Star all data, including email and files, continues to be owned by National Star. This data may be made available for business purposes to other staff following authorisation by the respective departmental or senior manager. Organisational and business information must not be retained by the individual once employment has ended.

3.9.5 The transfer of confidential information to recipients outside of the organisation such as Learner Health and Care Plans, medical information and Progress Reports must be implemented via a secure encrypted file transfer. IT service can advise on how to do this.

3.9.6 Staff must not attempt to load/save/access any data of a non-business nature onto National Stars IT Services. Doing so would increase the chance of cyber-attack or viruses. IT Services are not responsible for data loss of any personal files that have been stored within any National Star IT service.

3.9.7 When saving confidential documents to a shared space (e.g. Staff Shared Folder or the Intranet) the user must consider who has access to that location. Users who are unsure who else has access must check with the shared space owner or IT Services.

3.9.8 Portable devices such as phones, tablets and laptops whether National Star or personal owned 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 Devices' section in the policy for more information.

3.9.9 National Star laptops are all encrypted and on Issue the PIN number should be changed to one only the user knows. If issued to a team, the PIN number should be changed to one only the team knows. This number should be shared with the minimum number of staff, not shared with anyone who is not staff and not noted with the laptop (e.g. sticker or piece of paper).

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

3.9.11 National Star equipment or IT services must not be used to breach Copyright regulations or intellectual property rights.

3.9.12 If staff inadvertently accesses data/files that they believe that they should not have access to, they should notify the IT Services team immediately. Failure to do so could be deemed as a breach of this policy.

3.9.13 It is the responsibility of the user to ensure sensitive or confidential electronic information is only kept on encrypted removable media (e.g. memory sticks). Advice on encrypting removable media can be gained from the IT Services team.

3.9.14 Data must not be solely stored on the local computer, as it will not be backed up and could be wiped without warning. Where possible, data should be stored on the network (e.g. home drive, Intranet, shared drives) only. Where this is not possible due to software limitations, manual backups from the software must be taken after each change and saved to a networked location. This is to ensure all data is backed up to protect system failure, human error or cyber-attack.

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

3.10 Internet and eMail

3.10.1 National Star provides email and Internet services primarily for business, research, educational and communication purposes. However, as the organisation is committed to lifelong learning and development for all service users and staff, email and Internet access is not solely limited to work related activities.

3.10.2 Staff can have Internet and email access for limited non-business use outside of their working hours or during unpaid breaks providing those who need to work do not require the computers. Staff using National Star's IT Services are still representing National Star even when they are using these services for non-business purposes.

3.10.3 Whilst the National Star has taken reasonable action to prevent access to inappropriate content it should be noted that no such filtering system is perfect and will on occasion both allow access to inappropriate material and block access to legitimate material. If a user accidentally accesses inappropriate material they should inform IT Services team so a block can be manually introduced. No action will be taken against a member of staff for accidentally accessing inappropriate materials; such accidental access is clearly demonstrable in the internet logs.

3.10.4 National Star's IT services must not be used for personal political purposes or personal commercial business.

3.11 eSafety

We recognise service users with learning difficulties are potentially more vulnerable and more at risk than others when using ICT:

- Those with learning difficulties may make literal interpretations of content which will affect how they respond.
- They may not understand some of the terminology used.
- Those with more complex needs may not always understand the concept of friendship and therefore trust others naively.
- They may not know how to make judgements about what information is safe to share. This can lead to confusion about trusting others on the internet.
- Some service users may be vulnerable to being bullied or to extremism/radicalisation through the internet, and they may not be able to recognise this.
- Some service users may not appreciate how their own online behaviour may be seen by someone else as bullying.

National Star is committed to continuous professional development and training in computer use to ensure high levels of e-safety for both staff and service users.

3.12 Copyright

3.12.1 National Star respects and complies with copyright law. All users of the computer system must ensure that their use of the internet and materials taken from the internet complies with copyright law. Users must not download or attempt to download copyright material such as movies, games, music or software. Such activity is illegal and appropriate action will be taken against staff with pirate materials

or attempting to use National Star equipment to copy copyright materials will be subject to disciplinary action.

3.12.2 Provisions in the CDPA (Copyright Designs and Patents Act) permit educators and students to use and copy media for the purposes of instruction only.

3.12.3 Staff should not use pirated material for any activities. This includes music CD's, games, DVD's. Piracy is a crime and software piracy laws are being enforced by the government, police and the copyright holders. National Star can be audited without notice by trading standards to detect misuse.

3.13 Communications and Social Media

3.13.1 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.

3.13.2 Electronic communication including emails must be used in a professional manner. Communications must not contain statements or inferences which could be interpreted as either sexist, racist, extremist, harassing, libellous or in breach of legislation including Equalities legislation and the Prevent Duty guidance.

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

3.13.4 Users must immediately report to either a line manager or member of the HR team any email or other electronic communication that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

3.14 eMail

3.14.1 Email containing attachments and links should be treated with care, especially if they have come from an unknown sender. If in any doubt the email should not opened and advice should be sought from IT Services. This will prevent the spread of viruses via emails.

3.14.2 Protect other's email addresses when sending mail externally by using Blind Carbon Copy (BCC). When sending internal email to large number of people (e.g. All Staff) use BCC to prevent reply to all responses. If you require advice on how to do this please contact IT Services.

3.14.3 File attachments should only be sent when absolutely required. Do not send large attachments to multiple people. For internal recipients it is possible to state the path to the file on a shared drive or utilise the Intranet and send out a link to the file via email. If you require advice on how to do this please contact IT Services.

3.14.4 Emails should only be sent to recipients for whom it is relevant. Use email groups logically to keep communications to only necessary recipients. E mails sent to groups containing a large number of recipients e.g. 'All National Star Staff' maybe subject to approval by the group manager before delivery.

3.14.5 Staff should avoid sending emails containing jokes and 'chain letters' as such can been seen as unprofessional or inappropriate.

3.14.6 Email is not secure or private so confidential information being exchange with external parties must not be sent without first being encrypted. Do not include the decryption password in the email, it should be communicated to the intended recipient via alternative means such as telephone. If you require advice on how to do this please contact IT Services.

3.15 Social Media

Work-related use of social media

3.15.1 National Star recognises the importance of the internet in shaping public thinking about the charity, the services that are offered and the wider sector. The organisation also recognises the importance of staff joining in and helping shape conversations through interaction in social media.

Staff are permitted to interact on social media but must adhere to the following rules;

3.15.2 Before using work-related social media individual staff members must:

a) have read and understood this policy

b) have been authorised to post material on social media in the name of National Star, or on the organisation's behalf, by the Head of Communications.

c) have ensured that the correct permissions have been gained for the use of any images

If staff members have any doubt as to what can and cannot be said using social media, then either the Head of HR or the Head of Internal Communications should be contacted for clarification.

3.15.3 National Star permits the incidental use of social media for personal use in the workplace subject to certain conditions set out below. However, this is a privilege and not a right. It must neither be abused nor overused and the organisation reserves the right to withdraw permission at any time at the organisation's discretion.

The following conditions must be met for the personal use of social media:

a) use must be minimal and take place substantially out of normal working hours
b) use must not breach any of the rules set out in rules for using social media- Appendix C
c) use must not interfere with business or office commitments;
d) use must comply with other policies including the Equality & Diversity Policy, Safeguarding Policy, Data Protection Policy and Disciplinary Procedure.

3.15.4 Personal use of social media outside of work

Care should be taken not to blur the boundaries between work and personal life. All staff are responsible for their actions and should conduct themselves professionally. If an employee identifies themselves as a member of staff at National Star this has the potential to create perceptions about the organisation to both internal and external parties. The following guidance will apply where the use of personal communications impact on work activity.

Monitoring use of social media websites

3.15.5 Staff should be aware that any use of social media websites (whether or not accessed for work purposes) may be monitored. Where breaches of this policy are found, action may be taken under the Disciplinary Policy. Staff therefore must not invite or accept students as their 'friends' on Social Media.

3.15.6 National Star reserves the right to restrict or prevent access to certain social media websites if the organisation considers personal use to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

3.15.7 Misuse of social media websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against individual staff members and the organisation.

3.15.8 In particular uploading, posting forwarding or posting a link to any of the following types of material on a social media website, whether in a professional or personal capacity, will amount to gross misconduct (this list is not exhaustive):

a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit nature);

b) a false and defamatory statement about any person or organisation;
c) material which is offensive, obscene, criminal discriminatory, derogatory or may cause embarrassment to National Star, service users or staff;
d) confidential information about the charity, any staff member, service users (which you do not have express authority to disseminate);
e) any other statement which is likely to create any liability (whether criminal or civil, and whether for an individual staff member or the charity);
f) materials that are in breach of copyright or other intellectual property rights, or which invades the privacy of any person.

3.15.9 Where evidence of misuse is found, National Star will undertake a more detailed investigation in accordance with the Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary such information may be handed to the police in connection with a criminal investigation.

Staff noticing any breach of this policy through the use of social media should report it to the Head of HR.

4. ROLES AND RESPONSIBILITIES

4.1 Implementation

4.1.1 All staff members

Individual staff members are responsible for ensuring that they take the time to read and understand the policy and for ensuring their own compliance with it. Any breach should be reported to the Head of IT Services and Head of HR. Ensures that you follow the "E-Safety Flowchart" when an E-Safety concert occurs (Appendix B).

4.1.2 The Chief Executive

The Chief Executive is responsible for ensuring the safety (including e-safety) of members of the organisation, though the day to day responsibility for e-safety will be delegated to the Safeguarding Officer and Director of Technology Innovation.

4.1.3 SMT

The Senior Management Team will be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a service user or member of staff. (Appendix B) If there is the suspicion of illegal activity this may be elevated to the police or other appropriate authorities at the discretion of the Senior Management Team, Head of HR or Safeguarding Officer.

4.1.4 IT Services

The IT services team will be responsible for implementing the technical aspects of the policy and making recommendations to system improvements. They will also monitor and highlight any non-compliance detected. They will provide advice and training on how to undertake technical tasks required by this policy (e.g. encrypting pen drives, encrypting confidential data)

4.1.5 Head of IT Services

The Head of IT Services is responsible for ensuring the technical aspect of this policy are implemented and working as per the policy and the instructions of the senior management team. Has a leading role in establishing and reviewing the organisation's e-safety policies and documents.

4.1.6 Director of Technology Innovation

The Director of Technology Innovation holds SMT responsibility for this policy to ensure it is implemented. They are responsible for ensuing all other departments that need to deliver aspects of this policy are fulfilling their requirement. Ensures required training is in place. Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place (Appendix B).

4.1.7 Safeguarding Officers

The Safeguarding Officer is responsible for investigating alleged breaches of the policy with focus on e-safety. They will investigate breaches to the policy focused around Safeguarding.

They are trained in e-safety issues and need to be aware of the potential for serious child/adult protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

4.1.8 Head of HR

The Head of HR is responsible for investigating alleged breaches of the policy.

4.1.9 Head of Risk and Compliance

The head of Risk and Compliance is investigating alleged breaches of the policy with focus on Data Protection.

4.1.10 Training

- A planned programme of formal e-safety training is delivered as part of mandatory safeguarding training and will be made available to all staff and service users.
- An audit of e-safety, safeguarding and where relevant Prevent Duty training within the organisation will be carried out regularly as part of regulatory compliance activities.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the organisations Acceptable Use Policy.

4.1.11 Support, advice and communication

If further explanation or clarification is required, the individual must seek this from their line manager.

Support and training in undertaking technical tasks required by this policy (e.g. encrypting pen drives, encrypting confidential data) can be obtained from the IT Services team.

This policy will be communicated to all staff electronically or hard copy if required, Acceptance will be undertaken electronically prior to the users gaining access to IT services. Updates to this policy will be issued by requesting a reacceptance.

4.1.12 Review

The Head of IT Services and Director of Innovation Technology are responsible for leading the review of this policy, to ensure that it meets legal requirements and reflects best practice. Issues raised since the last policy review resulting from things that have changed or where greater clarification is needed will be incorporated. They will work with stakeholders around their respective areas of expertise, including the Safeguarding Officer, Head of HR, IT Services Team, Head of Risk and Compliance.

APPENDIX A – STAFF ACCEPTABLE USE POLICY DECLARATION

This declaration will be presented to the user and signed electronically prior to gaining access to IT services.

I have read the National Star **IT Acceptable Use Policy (AUP) - Staff** and I understand that:

I will comply with the Acceptable Use Policy and understand that breaches of this policy may result in IT access being suspended and may lead to disciplinary action up to and including summary dismissal.

National Star owns the IT systems and I understand that it is a criminal offence to use a computer system for a purpose not permitted by its owner.

I will use the college information systems professionally and in accordance with my role.

I will protect my user account password and will access IT services with my own user name and password. I will inform IT Services if I believe my password to have been compromised.

I will respect the IT security of others and not attempt to access files or accounts without authorisation.

I will respect IT systems settings and not try to install software or install or modify hardware without authorisation.

I will respect the security of IT systems and not knowingly use virus infected data.

I will conduct all electronic communication professionally

I will use internet services professionally and in accordance with the guidance in the Acceptable Use Policy

I will inform IT Services if I accidentally breach the Acceptable Use Policy.

I will observe copyright and intellectual property rights and law.

I will report any incidents of concern regarding child or adult protection and safeguarding to the Safeguarding Officer. This will be reported using procedure significant event form in line with the safeguarding policy and procedures.

I will ensure that all communications with service users are compatible with my role and meet the requirements of organisational policy.

I will follow the organisation's data protection policy and will ensure that personal data is kept secure and is used appropriately, whether at a National Star site, taken off the premises or accessed remotely.

I will promote the concept of 'e-safety' when working with service users.

All activity may be logged and will be monitored in accordance with the Acceptable Use Policy

I have read the Acceptable Use Policy and agree to work within the directive of this policy.

- To be accepted electronically prior to gaining access to IT services.

Acceptable Use Agreement (learners and residents)

This declaration will be presented or read to learners and residents and electronically acknowledged prior to gaining access to IT services.

This agreement is to help you:

- stay safe while using the internet and e-mail
- use IT properly
- use IT safely

IT = Information Technology which includes computers, laptops, tablets, smartphones, games consoles and communication aids.

Acceptable Use Agreement

For my own safety:

- I understand that my use of IT is logged and monitored
- I will not share my user name or password
- I will be aware of "stranger danger" when I am talking on-line
- I will report anything that makes me feel uncomfortable when I see it on-line
- I will be polite when I talk with others on-line. I will not use bad language. I understand that people may have different views and beliefs.
- I will not take or send pictures using the computer of anyone without their permission.
- I will not try to access material on the internet that is illegal or that will hurt the feelings of others
- I will report any damage to computers
- I will not open any attachments to emails, unless I know and trust the person who sent it (because of computer viruses)
- I will only use computer chat sites (Facebook) at times outside my normal working time unless I have permission.

When using the internet I know that:

- I will need to get permission to use the work of other people in my work
- I will not try to download music and videos that are copyright protected

I know that I am responsible for using computers properly

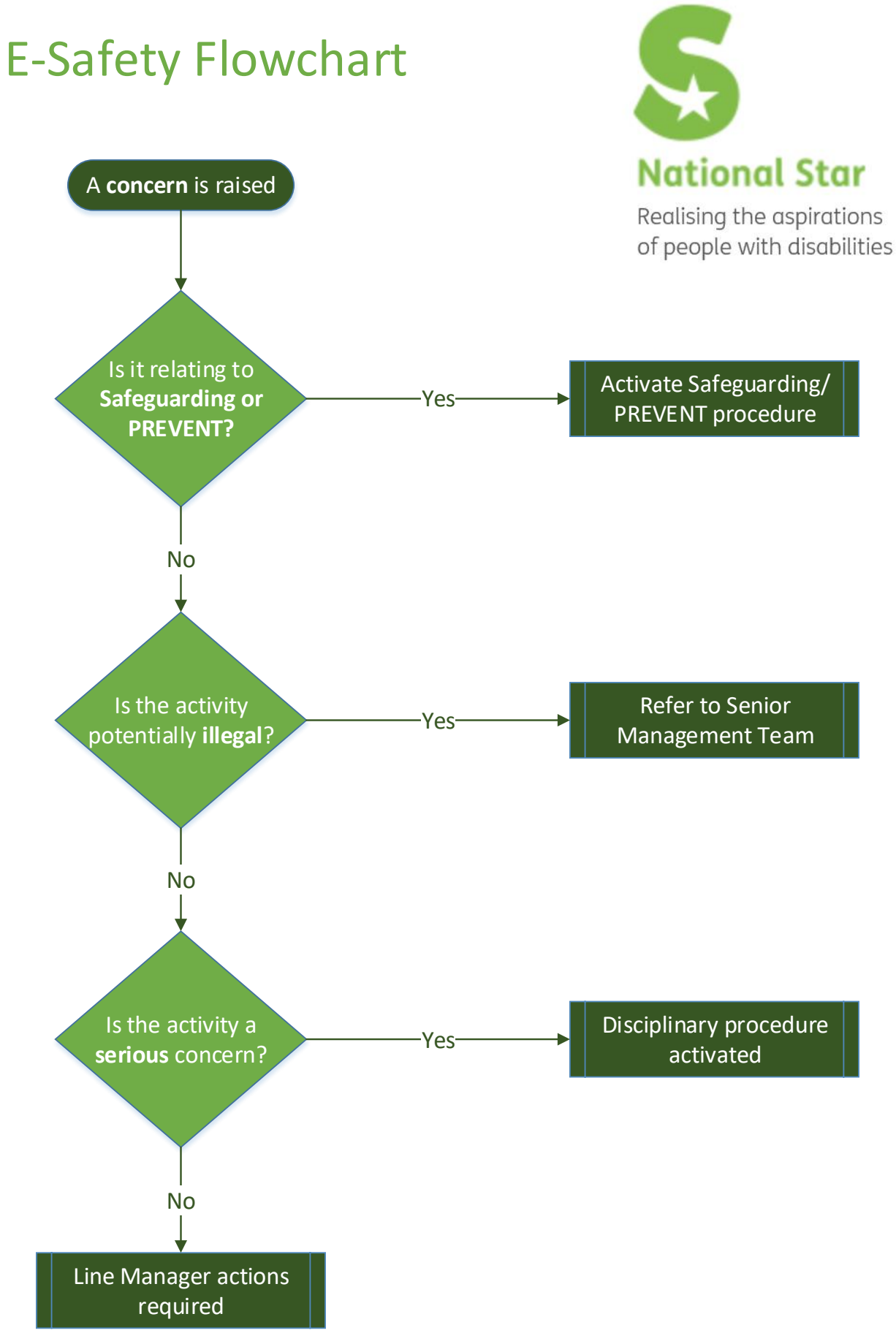
- If I do not use IT properly I may be stopped from using it or my parents or carer or the police may be informed.

Acceptable Use Agreement

I have read, or had read to me, the rules for using computers and agree to follow these rules when;

- I use IT in college or in my residence
- I use my own computer, communicator or smartphone
- I use my own computer to talk to other people – using e-mail or the Internet

APPENDIX B – E-SAFETY FLOWCHART



APPENDIX C – Rules for use of social media

Whenever staff are permitted to use social media in accordance with this policy, individuals must adhere to the following general rules:

- Always write in the first person, identify who you are and what your role is, and ensure that it is clear that the views expressed are your own and do not reflect the views of National Star.
- Ensure your actions will maintain National Star's reputation
- Do not upload, post, forward or post a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content or act in a way which might bring National Star into disrepute.
- Any member of staff who feels that they have been harassed or bullied, or are offended by material posted or uploaded by a colleague onto a social media website should inform the Head of HR
- Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with your line manager in the first instance.
- Do not upload, post or forward any content belonging to a third party unless you have that third party's express consent.
- Do not upload or live broadcast images, video or other media of service users without the prior consent of the communications team.
- When making use of any social media platform, you must read and comply with its terms of use.
- You are personally responsible for content you publish into social media tools, be aware that what you publish will be public for many years.
- Do not discuss or post images of colleagues, competitors, customers or suppliers without their prior approval.
- Staff must not accept or invite the following parties to be 'friends' on personal social media accounts or other online services: service users, parents (Note: Where former service users are 'friends' you should be mindful that they may have current service users as friends who may then have access to your details).
- Staff must conduct themselves in line with other organisation policies e.g. Equality and Diversity, Safeguarding
- Avoid publishing your contact details where they can be accessed and used widely by people you did not intend to see them, and never publish anyone else's contact details without their express consent.
- Activity on social media websites during working hours should complement and/or support your role and should be used in moderation.
- If you notice any content posted on social media about National Star, whether complimentary or critical, please report it to the Head of Communications.
- If any press or media interest is generated, refer this to Head of Communications.