ALAT and Bright Tribe Trust
ICT Monitoring Policy

Trust board approval date

August 2015

Contents

1. Mission Statement

Adventure Learning Academy Trust (ALAT) AND Bright Tribe Trust (Bright Tribe) brings a new energy and approach to providing the best education for our students. Through proven practices, ALAT / Bright Tribe will transform the learning of students, raise standards and provide the highest quality learning environments, enabling students and teaching staff to thrive and be the best. ALAT / Bright Tribe's aim is to break down the barriers that limit educational progress. We do this through adopting a personal learning pathway for every child – one that takes account of individual needs, aspirations and talents.

ALAT / Bright Tribe's values:

Learn	Grow	Prosper
Provide the best education for every student.	Grow our students' futures.	Lead the way in education.
Ensure the highest quality teaching and learning.	Develop the best teaching staff.	Realise the opportunities.
Work with the family, parent or carer.	Provide the best learning environment and supporting technology.	Be connected to the community.

2. ICT Monitoring including internet access and consent

ALAT/Bright Tribe are committed to ensuring that our whole community is safe and secure, and we take our responsibility to educate our staff and students on e-Safety issues very seriously. We will positively influence all of our community to be safe when using technology; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using ICT, in and beyond the context of the classroom.

3. Monitoring

In order for ALAT/Bright Tribe to successfully implement our community approach to e-Safety and Data Security, we feel that it is necessary for us to adopt a policy of monitoring. Whilst we respect the privacy of all members of our community, we also feel that it is very important that we are collectively empowered to prevent any incident where any member of our community may come to harm because of misuse of ICT equipment.

Authorised ICT staff may inspect any ICT equipment owned or leased by any member of the ALAT/Bright Tribe community at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification and contact the Director of Business Services. Any ICT authorised staff member will be happy to comply with this request.

Authorised ICT staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving the employees or contractors of ALAT/Bright Tribe, or any of our Member Academies, without consent, to the extent permitted by law.

This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of ALAT/Bright Tribe's ICT; for quality control or training purposes; to comply with a Subject Access

Request under the Data Protection Act 1998, or to prevent or detect crime.

Authorised ICT staff may, without prior notice, access the e-mail or voice-mail account where applicable, of a member of staff who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by Authorised ICT staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000. Please note that personal communications using ALAT/Bright Tribe's ICT resources may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

4. Purpose

4.1. The ICT Privacy and Monitoring Policy informs the Trust's staff, students, and other individuals entitled to use the Trust's facilities of how, and under what circumstances, monitoring of activity or inspection of the content of electronic data assets may be carried out.

4.2. Routine activity logging of the use of ICT based systems takes place to ensure the proper functioning of those systems and to guard against unauthorised activities, and this Policy formally authorises the Network Manager to inspect these logs within defined parameters.

4.3. The Policy also identifies the exceptional circumstances when a duly authorised representative of the Trust is permitted to monitor, without prior consent, an individual's activity (via examination of activity logs or examination of the contents of an individual's data assets, such as e-mails or personal document files).

5. Definitions

5.1. Activity logs: are a by-product of many IT based systems. In general, activity logs record that the user undertook an activity rather than the content of the activity e.g. that an e-mail was sent from A to B, but not what the content of the e-mail was.

5.2. Content Inspection: refers to the act of examining the content of an activity e.g. looking at the body of an e-mail message. Content inspection may be targeted or broad sweep.

5.3. Monitoring: refers to the process of examining activity logs and/or performing content inspection for a specific purpose.

5.4. Targeted: content inspection refers to the process of focussing these activities to an individual user or defined group of users

5.5. Broad Sweep: content inspection – i.e. not targeted at individuals is generally performed by automated processes designed to ensure the proper functioning and use of IT based systems. SPAM filtering is an example of broad sweep content inspection.

6. The ICT Privacy and Monitoring Policy

6.1. The Trust requires that staff, students and others making use of the Trust's ICT-based systems are aware that activity logging takes place, and that monitoring or content inspection of an individual's activity may occur under specific circumstances.

6.2. All activity logs will be properly secured and be compliant with the Trust's records management policy.

6.3. The Principal or appointed deputy is authorised to institute automated broad sweep monitoring and content inspection processes in order to ensure the proper functioning of IT systems, to validate

adherence to University policy, and to guard against unauthorised activities

6.4. The Principal or appointed deputy may authorise targeted monitoring and content inspection only under one or more of the following circumstances:

6.4.1. To establish specific facts, as part of a formal investigation, where a member of the Senior Leadership Team has reasonable grounds to suspect breach of Trust policy or to comply with the lawful request of a third party (e.g. the police or other government agency).

6.4.2. To ensure the effective operation of a service i.e. to understand why a system appears to be performing outside its normal operational tolerances

6.4.3. To enable access to information crucial to the running of the Academy or the Trust, in the absence of the individual.

6.4.4. Where targeted monitoring or content inspection is authorised, it must be carried out in accordance with the ICT Privacy and Monitoring Procedure (Appendix A) and in accordance with the principle of minimal access to information (i.e. information so derived will be strictly controlled and only be made available to authorised recipients).

6.5. Those members of Trust staff who have the capability to access activity logs or the electronics assets of others (e.g. systems administrators) must only exercise those abilities in the context of this policy.

6.6. Individuals in breach of this policy may be subject to disciplinary procedures at the instigation of the staff member with responsibility for the person concerned, in addition to potential prosecution under the Regulation of Investigatory Powers Act 2000.

7. Ownership

7.1. The Principal has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

Appendices

Appendix A: ICT Privacy and Monitoring Procedure

A.1 There are three reasons to request monitoring or content inspection of an individual's use of an IT system. They are:

A.1.1 To investigate a suspected breach of Trust policy or the law.

A.1.2 To access information crucial to the running of the Trust.

A.1.3 To ascertain why an IT system appears to be performing outside normal tolerances.

In the case of A.1.1 above, it may not always be appropriate or possible to inform the person(s) concerned.

In the case of A.1.2 above the person(s) concerned will be approached whenever possible prior to any third party access and will be informed as soon as possible afterwards.

In the case of A.1.3 above, the Principal or appointed deputy will establish basic facts and remedy without recourse to this procedure unless in so doing it becomes necessary under A.1.1 above.

A.2 For A.1.2 where a member of staff is absent, the line manager, with permission of the relevant senior member of staff, should seek permission to access the staff member's electronic assets, through direct dialogue with the member of staff. Contact should be made in accordance with the process for contacting staff at home.

A.3 The Principal or appointed deputy will arrange the approved access.

A.4 The Principal or appointed deputy will be responsible for ensuring that the access is revoked at the end of the specified period.

BrightTribe

learn grow prosper

Adventure Learning Academy Trust

CMA House 2nd Floor Newham Road Truro TR1 2SU

T 01872 858 161 **E** enquiries@alat.org.uk

www.alat.org.uk

Bright Tribe Trust

Building 1000 Kings Reach Yew Street Stockport SK4 2HD

Telephone 0161 475 0222 **Facsimile** 0161 831 9766 **Email** enquiries@brighttribe.org.uk

www.brighttribe.org.uk