The Active Learning Trust

INTERNET, SOCIAL MEDIA AND E-SAFETY ACCEPTABLE USE POLICY

This policy is reviewed on an annual basis

History of Document

Issue No	Author/Owner	Date Written	Approved by Trust Board	Comments
1	Director of Finance & Operations / DPO	May 2018	12 July 2018	1st formal issue

1. INTRODUCTION

1.1 The use of the Internet and social media has become an integral part of school life. The Active Learning Trust ("Trust") must embrace this for its opportunities, but also carefully manage its use to ensure appropriate protection for all users.

1.2 The Trust has an obligation to ensure persons using the Internet and social media in relation to School/ Trust activity, are absolutely clear about expectations regarding professional behaviour, protecting confidentiality of personal data and confidential information.

2. PURPOSE OF THE POLICY

2.1 The purpose of this Internet, Social Media and E-Safety Acceptable Use Policy ("Policy") is to outline the Trust's expectations for Internet and social media use.

3. SCOPE

3.1 This Policy is intended for anyone who has access to, uses, have control over or supports a school's social media or access to the Internet and explains the consequences of breaching acceptable use.

3.2 For this Policy definitions are as follows:

- Information covers any method of information creation or collection, including electronic capture and storage, video and audio recordings and any images.

- ICT or ICT system means computing and communications facilities that support teaching, learning and a range of activities in education.

- IT is the knowledge, skills and understandings needed to employ information and communication technology appropriately.

- Internet is a general term that covers access to numerous computers and computer systems worldwide that are accessed electronically.

- Social media is a type of interactive online media that allows parties to communicate instantly with each other, or to share data in a public forum. This includes online social forums such as Twitter, Facebook, Instagram, Snapchat, LinkedIn, Internet newsgroups, and chat rooms. Social media also covers blogs and video and image sharing websites such as YouTube and Flickr.

- Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the central operations of the Trust.

4. RESPONSIBILITIES

4.1 The Trust Board has ultimate responsibility for setting this Policy.

4.2 A Headteacher is responsible for ensuring that the requirements relating to this Policy are adopted and adhered to; the day to day management of Social Media arrangements, including delegating roles and monitoring effectiveness and has overall responsibility for the implementation of the Social Media arrangements in their school, must ensure it is implemented consistently and effectively, and is free from discrimination and subject to regular review.

4.3 The Designated Safeguarding Lead will educate staff on the safeguarding dangers associated with social media and online activity, have structures in place for use by concerned students and contribute to promoting an environment of safe and considered Internet use for all.

4.4 Employees must have an awareness of the terms of social media use for both themselves and their students, promoting the correct usage within their classroom environments and beyond.

4.5 ICT services are responsible for monitoring e-mail systems and social media to ensure data is protected.

4.6 Parents are responsible for upholding safe social media usage at home and reporting any concerns as appropriate.

4.7 Everyone who has access to a school's ICT systems and data must comply with this Policy, the Trust's ICT Security Policy and its Email Acceptable Use Policy. Anyone outlined in 3.1 above are required to read, accept and agree to abide with all these policies.

4.8 The Trust has produced IT Standards which cover its expected cyber security mechanisms and checks that schools must comply with in order to protect personal data as outlined by the General Data Protection Regulation.

4.9 An Information Management & Cyber Security Governance Group reports to the Trust's Senior Leadership Team and considers Trust wide cyber security and information management matters.

4.10 The Trust's Data Protection Officer and the Trust's Director of Finance and Operations are responsible for monitoring a school's compliance with the Policy; submitting a report on the effectiveness of the Policy (GDPR matters – the Data Protection Officer) and ICT matters (the Director of Finance and Operations) to the Trust Board as a minimum on an annual basis. The Trust's Data Protection Officer is responsible for submitting any reportable security breaches to the Information Commissioner's Office.

5. INTERNET

5.1 All use of the Internet at a school should be primarily to enhance teaching and learning or for administrative use. It is understood however that employees may occasionally need to use the Internet for personal reasons. Such use should be limited to outside of lesson time for teaching staff and during breaks/lunchtimes for support staff.

5.2 Staff must use caution when posting information on the Internet and must not post material damaging the reputation of a school/Trust which could cause concern about their suitability to work with students.

5.3 Staff posting material which could be considered inappropriate could render themselves vulnerable to criticism or allegations of misconduct.

5.4 Many Internet sites contain unacceptable contents. Employees must not deliberately view, copy or circulate any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material, the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains images, cartoons or jokes that will cause offence
- that constitutes bullying

5.5 A school records the details of all Internet traffic. This is to protect a school and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited. The logs record:

- the network identifier (username) of the user
- address of the Internet site being accessed
- where access was attempted and blocked by the system
- the Web page visited and its content
- the identity of the computer on the network and the date and time.

Data contained in these logs will be monitored regularly by the school's ICT service. Any excessive or inappropriate use could result in the facility being withdrawn or disciplinary action being taken. All monitoring information will be kept for six months.

5.6 Staff personal use of the Internet:

- Is limited to employees' own time
- Via school equipment should exclude use for trading or personal business purposes
- Buy goods or services will not render the school liable for default of payment or for the security of any personal information disclosed.

5.7 Many Internet sites that contain unacceptable content are blocked automatically by a school's filtering systems. However it is not possible to block all 'unacceptable' sites electronically in all circumstances. If staff become aware of any sites that require recategorisation they should inform a school's ICT service as soon as possible. Employees may receive an e-mail or visit an Internet site that contains unacceptable material. If this occurs, a line manager or the Headteacher should be informed as soon as possible. The Headteacher will use their professional judgement whether to report the matter further. In this situation the employee should ensure a short written record is kept as they may be asked to provide details relating to the incident and an explanation of how it occurred. This information may be required later for management or audit purposes.

5.8 Employees may be in violation of copyright law if text or images are simply cut and pasted into another document. This may equally apply to photographs and music samples used as illustration or backing track in resource materials. Teachers should make it clear to pupils that care should be taken when including this type of material in any school or exam work. Most sites contain a copyright notice detailing how material may be used. If in any doubt about downloading and using material for official purposes, legal advice should be obtained. Unless otherwise stated on the site all downloaded material must be for curricular or research purposes and must not be passed to third parties. Downloading of video, music files, games, software files and other computer programs – for non-work related purposes, is not allowed. These types of files consume large quantities of storage space on the system and may violate copyright laws.

6. SOCIAL MEDIA

6.1 Staff must use caution when posting information on social networking sites and blogs and must not post material damaging the reputation of a school/Trust which could cause concern about their suitability to work with students.

6.2 Employees posting material which could be considered inappropriate could render themselves vulnerable to criticism or allegations of misconduct. Staff must not be 'friends' to, or communicate with, students on 'Facebook', 'Myspace' and other social network or similar websites.

6.3 Employees must not:

- Damage the school's reputation on social media at work or within their own time. This includes on their own or school owned technology, by criticising or insulting students, staff, parents, relevant third parties, figures in the community or the site;
- Discuss school matters through social media, or share confidential information regarding colleagues or students;
- Adhere to, 'share' or 'like' potentially offensive material or pages, or promote criminal activity;
- Post content or opinions deemed racist, sexist, homophobic or hateful;
- Carry out cyber bullying or intimidating behaviour;
- Publicise personal conversations, link to personal sites or disclose private emails; and
- Post inappropriate images.

6.4 Under no circumstance should students be in contact with employees through social media. Any correspondence received should be reported to the Designated Safeguarding Lead. Students under the age of 18 who have left a school should not be befriended and caution urged beyond this age.

6.5 Employees are encouraged to report inappropriate behaviour online if they witness, or believe it to be being conducted, by a member of staff. Inappropriate behaviour involving a child or students **must be reported.**

6.6 Employees are highly advised to have the privacy settings on the highest setting if they choose to have a presence on social media sites.

6.7 Employees are reminded not to assume their conversations on social media sites are confidential or secure and not to share personal information, such as their home address.

7 E-SAFETY

7.1 Whilst access to unsuitable Internet content is minimised by filtering software, this can never be completely eliminated. It is therefore important that employees recognise their duty of care to ensure that students do not access or search for inappropriate website content.

7.2 Students should not give out personal information online (including through e-mail).

7.3 For reasons of child protection, student data and photographs should not be stored online unless in a secure area. This includes on a school's Virtual Learning Environment.

7.4 If a User suspects that illegal content has been accessed on a computer, the workstation should be immediately powered down and secured. Users should not attempt to check whether content is illegal by accessing it and a school's Headteacher should be contacted immediately.

8 CYBERBULLYING

8.1 Cyberbullying can be perpetuated through social media in a number of combinations. Intimidating language, threats, abuse, harassment, belittling or mockery perpetuated by students or staff in a sustained manner through social media platforms is unacceptable. Whether this is carried out during school hours is irrelevant.

8.2 Students and employees are aware that harassment, bullying and/or abuse perpetrated through digital platforms is incredibly serious and will be treated as such. Reports will be taken seriously and investigated, with the potential to progress to sanction and disciplinary action.

9 MONITORING

9.1 The contents of school/Trust ICT resources and communications systems are Trust property. Therefore all Users should have no expectation of privacy in any email communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

9.2 The Trust reserves the right to monitor, intercept and review, without prior notification or authorisation from adults, our email systems to monitor whether the use of the e-mail system is legitimate and in accordance with this Policy:

- to assist in the investigation of alleged wrongful acts; or
- to comply with any legal obligation

9.3 The Trust reserves the right for appropriate employees to use approved software tools to monitor emails in accordance with applicable laws and policies.

9.4 Suspected or actual security breaches are to be reported to a Headteacher who in turn will notify the Trust's Data Protection Officer in accordance with the Trust's Data Protection Policy. The right to monitor communications includes messages sent or received by system users (employees, volunteers, students) within and outside the system as well as deleted messages.

9.5 An annual information security/data protection monitoring programme will be undertaken to evidence the effectiveness of this Policy. Evidence will be obtained in order to meet the accountability principle of the General Data Protection Regulation.

10. DISCIPLINARY ACTION

10.1 Accessing inappropriate and indecent materials from the Internet or via e-mail may result in disciplinary action being taken. Employees must use caution when posting information online including on social networking sites.

10.2 Breaches of this Policy may constitute gross misconduct and as such may lead to staff dismissal. For individuals not directly employed by the Trust, breaches of the Policy may result in withdrawal of facilities and referral made to their employer. For all other adults breach of this Policy may be a breach of the Code of Conduct and may lead to sanctions being applied up to and including their removal from the Governing Bodies.

10.3 The Police will be informed where there is a possibility that a criminal offence has been committed.

10.4 If an employee is aggrieved or wishes to register or report a complaint they must follow the Trust's Whistleblowing Policy and/or Staff Grievance Procedures.

11. REPORTING

11.1 The Trust's Director of Finance and Operations is responsible for submitting a report on the effectiveness of this Policy to the Trust Board as a minimum on an annual basis.

12. REVIEW

12.1 This Policy will be reviewed on an annual basis by the Trust Board.