Arthur Terry Learning Partnership

Policy: ATLP E-Safety Policy

Aim: Document to demonstrate the Arthur Terry Multi-Academy Trust's policy with regards ICT and E-Safety

Document Control

Author/Contact:	ATLP IT Strategy Group / michelle.doughty@atlp.org.uk claire.cheswick@atlp.org.uk	
Document Reference:	E-Safety Policy	
Version	0.1	
Status	Final	
Publication Date	February 2020	
Related Policies	School policies – Anti-Bullying Policy, Behaviour Policy and Home School Agreement, relevant Marking and Assessment/Feedback Policies ATLP Policies – Staff Acceptable Use Policy, Student Acceptable Use Policy, Complaints Policy, Safeguarding Policy	
Review Date	February 2022	
Approved/Ratified By	Trust Board	Date: 3/2/2020

1. Introduction

The Arthur Terry Learning Partnership (ATLP) ICT services:

- Contribute to high quality teaching and learning
- Enables effective tracking, target setting and the management of intervention strategies
- Enables focused assessment
- Supports effective internal and external communication

However, there are inherent dangers of using this powerful tool in a school environment. It is therefore essential that schools create a safe ICT learning environment that includes three main elements:

- An effective range of technological tools
- Policies and procedure to describe and maintain the acceptable use of the schools ICT services and facilities with clear roles and responsibilities
- A comprehensive e-Safety education programme for students, staff and parents.

The e-Safety Policy has been written in accordance with our vision for the ATLP and is supported by the following school policies:

Anti-Bullying Policy, Behaviour Policy and Home School Agreement, Safeguarding Policy, Complaints Procedure and relevant Marking and Assessment/Feedback Policies

2. Key Principles

The ATLP has a number of key principles that apply to teaching and learning from and ICT and E-Safety perspective:

- All students should be able to learn in a safe environment and should not be exposed to inappropriate materials or cyber-bullying
- All staff are responsible for promoting and supporting safe behaviours in their classrooms and following the ATLP's e-Safety policy
- There is a 'No Blame' culture so students feel able to report any bullying, abuse or inappropriate materials for investigation.

3. Aims

The ATLP has a number of key aims that apply to teaching and learning from and ICT and E-Safety perspective:

- To ensure students can learn in a safe and secure environment, in and out of school
- To minimise the risk of student exposure to inappropriate material or cyber-bullying

- To develop secure practice for students when communicating electronically
- To develop student self-responsibility when communicating electronically
- To ensure consistent good practice for staff when communicating electronically
- To ensure all staff are aware of issues relating to e-Safety
- To provide information, advice and guidance for parents/carers on the use of new technologies.

4. Roles and Responsibilities

Trust Board

- Ensures that the e-Safety Policy is implemented, monitored and reviewed

ICT Strategy Group

- Ensure, along with the Trust Board, that the e-Safety Policy is implemented, monitored and reviewed.
- Ensure that all staff are aware of their responsibilities under the policy and are given appropriate training and support so that they can fulfil their responsibilities
- Ensure that issues of e-Safety, including cyber-bullying, are addressed within the curriculum

ATLP Safeguarding Staff

- Ensure that the Trust remains 'up to date' with e-Safety issues and guidance through organisations such The Child Exploitation and Online Protection (CEOP)
- Ensure that each Head teacher is updated as necessary, including being aware of local and national guidance on e-Safety and they are updated at least annually on policy developments

ATLP ICT Service

- Ensure the Trust Network is safe and secure for all groups – consistent application of protocols and management and development of software
- Advise ICT Strategy Group on e-Safety issues/technology

Teachers/Tutors/mentors/teaching assistants

- Responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures

5. The Trust ICT System

The security of the Trust ICT System is maintained by:

- Ensuring its health through appropriate management of appropriate security services (e.g. Anti-virus Service).
- Ensuring it is 'healthy' though robust monitoring of network use.
- Ensuring the ICT Team is up-to-date with providers services for security.
- Ensuring that the filtering methods are effective in practice and that access to any website considered inappropriate by staff is removed immediately.
- Using individual log-ins for students and all other users.
- Never sending personal data over the Internet unless it is encrypted or otherwise secured.
- Ensuring students only publish within appropriately secure learning environments such as their own closed secure log-in or Office 365.

6. The Internet

The ATLP recognises that access to the Internet is an invaluable learning tool and is vital for effective communication. Safety and security risks are minimised through:

- The supervision of students using the Internet within school at all times, as far as is reasonable, and vigilance in learning resource areas where students have more flexible access.
- The use of internal filtering systems which block sites that fall into categories such as pornography, race hatred, gaming, other sites of an illegal nature.
- Effective planning - Internet use is matched to students' ability.
- Informing users that Internet use is monitored in the Acceptable Use Policy, and as part of our student induction process in ICT lessons.
- Informing staff and students that that they must report any failure of the filtering systems directly to the ATLP ICT Service.
- Blocking all social networking sites except those that are part of an educational network.
- Only using approved 'Blogging' or discussion sites.
- Require students (and their parent/carer) to individually sign an ATLP Acceptable Use Policy, which is used as part of the teaching programme. A copy is kept on file, and this ensures parents provide consent for students to use the Internet, as well as other ICT technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school.
- Requiring all staff are made aware of the ATLP Acceptable Use policy and that on signing their terms and conditions of employment they agree to comply with its contents.
- Ensuring all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.
- Maintaining a record of any cyber-bullying or inappropriate behaviour (the e-Safety Log and the Behaviour Log) and act to deal with the perpetrators of this behaviour.
- Making information on reporting offensive materials, abuse/bullying etc. available for students, staff and parents.
- Immediately referring any material suspected of being illegal to the Police.

- Establishing that email and Internet use is not private and the schools reserve the right to monitor all emails and Internet usage involving the school's IT facilities and/or services.
- Allocating an email account through one of the Trust domains – enabling them to access their email from school and at home.
- Ensuring staff do not communicate with students via their personal email accounts or through their personal social networking site account (e.g. Facebook, Twitter etc.).
- Ensuring staff only communicate with students via their designated School email account.
- Ensuring staff do not attempt to use their personal social networking site(s) in school.
- Ensuring staff do not communicate with, or have details of, students on their personal social networking account or any other electronic device.
- Ensuring that staff should not have student contact details on their personal mobile phones; except for the specific duration of a school trip/visit.
- Ensuring that student details are always taken from the MIS system, and any new contact details obtained being passed to the school office for updating as may be appropriate.
- Making students aware of the risks and issues associated with communicating through email and to have strategies to deal with inappropriate emails, as part of the school's e-Safety and anti-bullying education programme.

7. Digital and Video Images

To prevent the inappropriate use of images of students within the ATLP the following is observed:

- Due to the new GDPR Regulations, images of students will only be used if consent has been provided by either the parent/carer or student themselves (this is dependent on whether the student is age 12/13 years). No images of students will be used on any external site if written consent has not been provided.
- Photographs published on the Internet will only have names if consent has been provided.
- Digital images /video of students are stored securely on ATLP approved systems and devices only.
- Students' names are not used when saving images in the file names or in the <ALT> tags when publishing to the school Website.
- Head Teachers take overall editorial responsibility for the website but delegate the operational day to day management to a named individual to ensure content is accurate and quality of presentation is maintained.
- Uploading of information is delegated to individuals responsible for specified areas.
- The Trust and each school's website comply with the Ofsted guidelines.
- Where other's work is published or linked to, the school credits the sources used and state clearly the author's identity or status.
- The point of contact on the Website is each school's main address and telephone number. Home information or individual private email identities will not be published.
- Staff are made aware of the Acceptable Use Policy.
- Students are taught to be aware of the possible wide range of audiences and how images can be abused in their e-Safety education programme.

8. Cyber Bullying

The use of the Internet, text messages, email, video or audio to bully another student or member of staff will not be tolerated. Bullying can be done verbally, in text or images e.g. graffiti, text messaging, Email or postings on websites.

'Cyber bullying' is a form of bullying via communication technology like text messages, email or websites. It takes many forms - sending threatening or abusive text messages or email, personally or anonymously, making insulting comments about someone on a website, social networking site (e.g. Facebook) or online diary (blog/Twitter), making, or sharing, derogatory or embarrassing videos of someone via mobile phone or Email (such as 'Happy Slappy' videos).

It should be noted that the use of ICT to bully could be against the law. Abusive language or images used to bully, harass or threaten another, whether spoken or written (through electronic means), may be libellous and contravene the Harassment Act 1997 or the Telecommunications Act 1984.

The nature and consequences of cyber-bullying are addressed through the curriculum. A range of strategies are recommended to support someone who is the victim of cyber-bullying.

9. Monitoring Arrangements

Appropriate monitoring arrangements in relation to all Internet, email and related services and facilities that it provides are in place and the Trust will apply these monitoring arrangements to all users. These arrangements may include checking the contents of, and in some instances recording, email messages for the purpose of:

- Establishing the existence of facts relevant to schools within the ATLP
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of email facilities
- Ensuring effective operation of email facilities
- Determining if communications are relevant to the School, for example where an employee or student is off sick or on holiday.

The Trust may, at its discretion, apply automatic message monitoring, filtering and rejection systems as appropriate, and deny transmission of messages with content that is unacceptable in the terms of this Policy.

These monitoring arrangements will operate on a continual and continuing basis, with the express aim of monitoring compliance with the provisions of the school's e-Safety Policy and for the purposes outlined above as permitted by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

The Trust will arrange for an appropriate disclaimer to be appended to all email messages that are sent to external addresses from the school, in order to provide necessary legal protection.

10. e-Safety Education

Students

An e-Safety programme is provided for all students on

- How to stay safe
- Social media
- Cyber bullying

At all Key Stages e-Safety forms a component of the assemblies.

10.2 Staff

All staff are required to read the e-Safety Policy and the Acceptable Use Policy. E-Safety updates are circulated when received

10.3 Parents/Carers

E-Safety Information is provided for parents. Advice and guidance can also be accessed via the Trust Websites.

11. e-Safety Complaints

11.1 Role of School

Complaints should be dealt with in accordance with the ATLP Complaints Procedure. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

Complaints related to safeguarding are dealt with in accordance with the ATLP Safeguarding Policy.

The schools take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a schools computer or mobile device. The schools cannot accept liability for material accessed, or any consequences of Internet access or ICT usage.

11.2 Investigation of Complaints

The school will investigate complaints received from both internal and external sources, about any unacceptable use of ICT that involves the school IT facilities.

External complaints will be addressed with reference to our Complaints Policy.

The investigation of facts of a technical nature, e.g. to determine the source of an offending email message, will be undertaken by the ATLP Operations & Estates and IT Team, in conjunction with other departments as appropriate.

Where there is evidence of a criminal offence, consideration will be given to whether the issue will be reported to the police for them to take appropriate action. The schools will co-operate with the police and other appropriate external agencies as required in the investigation of alleged offences.

In the event that the investigation of the complaint establishes that there has been a breach of the standards of acceptable use, then appropriate action will be taken.

11.3 Action in the Event of a Breach of the Standards of Acceptable Use

In circumstances where there is assessed to be a breach of the standards of acceptable use, the schools will, as a first action, act promptly to prevent continuance or repetition of the breach, for example to withdraw any unacceptable materials. This action will be taken in accordance with the normal managerial arrangements and will typically involve liaison between the appropriate member(s) of the Leadership, ATLP Operations & Estates and IT teams.

Subsequent action will be as described below:

- Indications of non-compliance with the provisions of the e-Safety Policy will be investigated, as appropriate, in accordance with the provisions of the school's Disciplinary Procedures, as applicable to staff and students
- Subject to the findings of any such investigation, non-compliance with the provisions of the e-Safety Policy will lead to appropriate disciplinary action, which could include dismissal on the grounds of gross misconduct for staff members or exclusion for a student. Furthermore, publication, accessing or storing of some materials may not only amount to a disciplinary offence, but also a criminal offence, in which case the issue will be reported to the police for them to take appropriate action
- Complaints of cyber-bullying will be included be recorded and dealt with in accordance with our Anti-Bullying Policy
- Complaints related to child protection are dealt with in accordance with the schools child protection procedures
- In the case of child pornography being found, the person or persons suspected should be reported immediately to ATLP Head of HR and the Police will be called.
- Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP): http://www.ceop.gov.uk/reporting_abuse.html.