CHILDWALL
SPORTS &
SCIENCE ACADEMY

# e-Safety Policy

CHILDWALL
SPORTS &
SCIENCE ACADEMY

LYDIATE
LEARNING TRUST

# E-SAFETY POLICY

## Table of Contents

# e-safety Policy

## Rationale

The e-Safety policy sets out the framework and expectations that all staff, learners and the academy community should adhere to in respect to the use of computing equipment, the internet and all forms of electronic communication such as email, mobile phones, portals/intranets, social media sites and related learning technologies.

The e-Safety policy is designed to detail the principles all users should adhere to when using these services. This guidance does not attempt to cover every possible situation but should be used as a supporting framework in relation to e-Safety.

## 1. Introduction

Childwall Sports & Science Academy (CSSA) recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide safe and secure internet access to all learners and staff and encourage the use of ICT and learning technologies in order to enhance skills, promote achievement and enable lifelong learning and world class outcomes.

However, the accessibility and global nature of the internet and associated learning technologies that are available mean that we all need to be aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the academy while supporting staff and learners to identify and manage risks safely, independently and with confidence.

We believe this can be achieved through a combination of security measures, training, guidance and the implementation of the relevant policies. In addition to our duty to safeguard staff and learners and the Every Child Matters agenda, we will do all that we can to make our staff and learners and e-Safe and to satisfy our wider duty of care. The e-Safety policy should be read alongside the following associated AET policies:

Staff Acceptable User Policy (AUP)
Student AUP
Electronic Information & Communications Systems Policy
Data Protection Policies Human Resources Policies CCTV Policy

From Ofsted's perspective, e-Safety is a critical part of the inspection process. The table below details the key features found when good or outstanding e-Safety practice is in place.

| | |
|---|---|
| Whole school consistent approach | All teaching and non-teaching staff can recognise and are aware of e-Safety issues.<br>High quality leadership and management make e-Safety a priority across all areas of the school (the school may also have achieved a recognised standard, for example the e-Safety Mark).<br>A high priority given to training in e-Safety, extending expertise widely and building internal capacity.<br>The contribution of students, parents and the wider school community is valued and integrated. |
| Robust and integrated reporting routines | School-based online reporting processes that are clearly understood by the whole school, allowing the students to report issues to nominated staff, for example SHARP.<br>Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support. |
| Staff | All teaching and non-teaching staff receive regular and up-to-date training. At least one staff member has accredited training, for example CEOP, EPICT. |
| Policies | Rigorous e-Safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by governors.<br>The e-Safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying.<br>The e-Safety policy should incorporate an Acceptable Usage Policy that is signed by students and/or parents as well as all staff and respected by all. |
| Education | A progressive curriculum that is flexible, relevant and engages students' interest; that is used to promote e-Safety through teaching students how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.<br>Positive rewards are used to cultivate positive and responsible use. Peer mentoring programmes. |
| Infrastructure | Recognised Internet Service Provider or RBC together with age/maturity related filtering that is actively monitored. |
| Monitoring and Evaluation | Risk assessment taken seriously and used to good effect in promoting e- Safety. Using data effectively to assess the impact of e-Safety practice and how this informs strategy. |
| Management of Personal Data | The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 2018. |

## 2. Creation, Monitoring and Review

The e-Safety Policy has been prepared with guidance from DfE Principles of e-Safety and previous CSSA e-Safety Policies and advice.

An annual review of the e-Safety policy is carried out by a group in the academy that includes the Data Manager, the child protection officer, a senior leadership team representative, a member of the ICT support team.

The impact of this policy will be monitored regularly with a full review being carried out at least once a year. This policy will also be reconsidered where particular concerns are raised or when an e-Safety incident has been recorded.

## 3. Policy Scope

The e-Safety policy applies to all users, learners, staff and all members of the academy community who have access to the academy ICT systems, both on the premises and remotely. Any user of the academy ICT systems must adhere to and sign a hardcopy of the appropriate ICT Acceptable User Policy. The e-Safety Policy applies to all use of computing equipment (fixed and mobile), the internet and all forms of electronic communication such as email, mobile phones, portals/intranets and social media web sites.

## 4. Roles and Responsibilities

There are clear lines of responsibility for e-Safety within the academy. The first point of contact should be the Data Manager. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager and the Data Manager. All teaching staff are required to adhere to this incident reporting procedure.

## 4. Roles and Responsibilities

There are clear lines of responsibility for e-Safety within the academy. The first point of contact should be the Data Manager. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager and the Data Manager. All teaching staff are required to adhere to this incident reporting procedure.

When informed about an e-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. All learners must know what to do if they have e-Safety concerns and who to talk to. In most cases, this will be the Data Manager or the Child Protection Officer. Where any report of an e-Safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Child Protection Officer may be asked to intervene with appropriate additional support from external agencies.

Listed below are the roles and responsibilities that should be in place in the academy/ are referred to in the e-Safety Policy:

**Data Manager**

The Data Manager and the ICT Team are responsible for keeping up to date with new technologies and their use, as well as attending any relevant training. They will be expected to lead the e-Safety agenda, review the e-Safety Policy, deliver staff development and training, manage the reporting procedure, record incidents, report any developments and liaise with the LLT and external agencies to promote e- Safety within the academy community. They may also be required to deliver workshops for parents.

**Learners**

Learners are responsible for using the academy ICT systems, mobile devices and learning technologies in accordance with the e-Safety Policy and the academy student AUP which they must sign at the time of registration at the academy. Learners must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. They are responsible for attending e-Safety lessons as part of the curriculum and are expected to know and act in line with other relevant academy policies for example; mobile phone use, sharing images, and cyber-bullying. They must follow the reporting procedures where they are worried or concerned, or where they believe an e-Safety incident has taken place involving them or another member of the academy community.

**Staff**

All staff are responsible for using the academy ICT systems, mobile devices and learning technologies in accordance with the e-Safety Policy and the staff AUP which they must sign and submit to the Data Manager. Staff must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. Staff are responsible for attending training on e-Safety and displaying a model example to learners at all times through embedded good practice.

All digital communications with learners must be professional at all times and be carried out in line with the Electronic Information and Communications Systems Policy. Online communication with learners is restricted to academy provided systems. External platforms not hosted by the academy (for example social media sites) may only be used where a risk assessment has been completed by the member of staff and submitted to the Data Manager and Headteacher for approval.

All staff should adhere to the relevant academy policies detailed in the e-Safety Policy and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the Data Manager, HOF for ICT for the ICT Team without delay.

## 5. Security

The academy will do all that it can to make sure the academy ICT network and systems are safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and firewalls for servers, routers, and all academy provided user devices (desktop/laptop/tablet/mobile etc.) to prevent accidental or malicious access of academy systems and information.

Digital communications, including the academy network, the Google Apps for Education platform, email systems, document storage and academy portals/intranets may be monitored in line with the Data Protection Policies.

CSSA have implemented, for security purposes that all user account passwords be changed on a 180 day cycle.

## 6. Risk Assessment

In making use of new technologies and external online platforms, all staff must first carry out a risk assessment for e-Safety. This consists of a series of questions for the requestor to answer as well as a section in which they can record any relevant comments or evidence. A risk assessment must also be carried out where a learner is learning off site e.g. on work placement. All forms must be submitted to the Data Manager for his/her consideration and approval.

## 7. Behaviour

Online communication can take many forms, whether it is by email, text, webcam or instant chat. It is essential that all staff and learners are aware of the academy policies that refer to acceptable behaviours when communicating online.

- the academy will ensure that all users of technologies sign and adhere to the standard of behaviours set out in the staff and student AUPs.
- the academy will not tolerate any abuse of its ICT network, infrastructure or cloud based systems, whether offline or online. All communications by staff and learners should be courteous and respectful at all times as details in the Electronic Information and Communications Systems Policy.
- any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes (available on the web site).

## 8. Communications

The academy requires all users of ICT to adhere to the appropriate staff and student AUPs which states clearly when email, mobile phones, social media sites, games consoles, chatrooms, video conferencing and web cameras may or may not be used during the academy day. Any required change or extension to these charters will require the permission of the Headteacher with advice provided by the Data Manager.

## 9. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

All staff and learners should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. LLT General Data Protection Regulations (GDPR) will apply alongside the CCTV Policy.

Academy teaching staff will provide information to learners on the appropriate use of images. This includes photographs of learners and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. Photographs of activities on the academy premises should be considered carefully and have the correct consent before being published. Approved photographs should not include names of individuals without consent. The CCTV policy will apply.

## 10. Personal Information

Personal information is information about a particular living person. The academy collects and stores the personal information of staff and learners regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The academy will keep that information safe and secure and will not pass it onto anyone else without the express consent of the individual or learners' parent/carer as appropriate as in line with the LLT GDPR Policy.

No personal information can be posted to the academy website unless it is in line with the LLT GDPR Policy. Only names and work email addresses of staff will appear on the academy website and no learners' personal information will be available on the website without consent and compliance with the LLT GDPR Policy.

Policies.

Staff must keep learners' personal information safe and secure at all times. When using any online or cloud platforms, all personal information must be password protected. No personal information of individuals is permitted off-site unless the member of staff has the written consent from that individual and the written permission of the Headteacher.

Every user accessing the academy ICT systems and services both onsite or remotely is required to log off on completion of any activity, or where they are physically absent from a device for any period. All academy mobile devices such as a laptops, tablets or mobile devices are required to be encrypted, password protected and signed out by the Data Manager or a member of the ICT staff before leaving the premises. Where any personal data is no longer
required, it must be securely deleted in line with the LLT data protection policies.

The use of USB's is banned for staff and students. Use of One Drive is encouraged.

## 11. Education and Training

With the current unlimited nature of internet access, it is impossible for the academy to eliminate all risks for staff and learners. It is our view therefore, that the academy will support staff and learners stay e-Safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

**For learners**

Learners will attend e-Safety lessons with the first of these will taking place at the beginning of each new academic year, with follow up lessons carried out via the curriculum.

Issues associated with e-Safety apply across the curriculum and learners will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.

Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. A link to the academy e-Safety Policy will be available on the academy network and with the rules highlighted in posters and leaflets around ICT areas and classrooms. Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

**For staff**

Resources and useful guidance and information will be issued to all staff as and when required. Each member of staff must inform the main office of the date of the training attended so that it can be recorded on SIMS.

Any new or temporary staff users will receive training on the academy ICT network system and Google Apps for Education platform led by the ICT Manager. They will also be asked to sign the Staff AUP.

## 12. Incidents and Response

Where an e-Safety incident is reported to the academy this matter will be dealt with very seriously. The academy will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor/teacher or to the academy Data Manager.

Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, the academy will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the staff AUP.

Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

## 13. Feedback and Further Information

The academy welcomes all constructive feedback on this and its linked policies. If you would like further information on e-Safety, or wish to send us comments on our e-Safety Policy, then please contact:

Academy Data Manager: Mrs S Sweeney

or the Academy Headteacher: Ms J E Vincent

## 14. Appendices

### 14.1 Data Protection

The Data Protection Act 2018 prohibits the disclosure of personal data except in accordance with the principles of the Act. This prohibition applies to Email in the same way as to other media. Information gathered on the basis that it would be seen by specified employees must not be given to a wider audience. In accordance with the provisions of Article 8 of the European Convention on Human Rights[1], the LLT/Academy respects the right to privacy for employees who use IT equipment but does not offer any guarantee of privacy to employees using IT equipment for private purposes.

As data controller, the Academy has responsibility for any data processed or stored on any of its equipment. Any employee monitoring will be carried out in accordance with the principles contained in the Code of Practice issued by the Information Commissioner under the provisions of the Data Protection Act 2018.

In order to comply with its duties under the Human Rights Act 1998, the LLT/Academy is required to show that it has acted proportionately, i.e. are not going beyond what is necessary to deal with the abuse and that the need to investigate outweighs the individual's rights to privacy, taking into account the LLT / Academy wider business interests. In drawing up and operating this policy the Academy recognises that the need for any monitoring must be reasonable and proportionate.

Auditors (internal or external) are able to monitor the use of the AET/Academy IT equipment and the storage of data. They are nevertheless bound by the provisions of the Human Rights Act 1998, the Data Protection Act 2018, associated codes of practice and other statutory provisions and guidance, including the Regulation of Investigatory Powers Act 2000 in respect of any activity that could be classed as directed surveillance