Longsands Academy

E-Safety Policy

Date	October 2021
Written by	Clare Greaney, Vice Principal Designated Safeguarding Lead
Approved by Longsands LGC	October 2021
Review Date	September 2023

Introduction and Aims

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet. Please also refer to Longsands Safeguarding Policy and Longsands Positive Behaviour Management Policy.

The internet and other technologies have opened up new opportunities for everyone as they are such powerful tools in our day to day lives. New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside the Academy. Electronic communication helps teachers and students learn from each other by increasing knowledge, promoting discussion and stimulating creativity. Children and young people should have an entitlement to safe internet access at all times. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. Whilst the use of these exciting and innovative tools in the Academy and at home plays a part in raising educational standards and promoting student achievement, the use of these technologies can put young people at risk within and outside the Academy. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Behaviour, Safeguarding and our guidance around mobile phone use.

It is impossible to eliminate risks associated with on-line activities completely, however, good educational provision which builds resilience to the risk that students might be exposed to will help to mitigate these and will provide them with the confidence and skills to deal with any concerns. At Longsands we work hard to educate students around the risks of the on-line world and do everything we can to help students to learn how to manage and reduce those risks.

Our e-safety policy explains how the Academy intends to do help our students to manage risks on-line, whilst also addressing wider educational issues in order to help young people (and

parents/carers/staff) to be responsible users and stay safe while using the internet and other communications technologies both in and out of the Academy.

Extent of the Policy

This policy applies to all members of the Academy community (including staff, students, parents/carers and visitors) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of students when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of the Academy, but is linked to being a member of our Academy community. The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate on-line behaviour that take place out of the Academy.

Principal & Senior Leadership Team (SLT)

The Principal is responsible for ensuring:

- The safety (including e-safety) of all members of the Academy community.
- Adequate training is provided.
- Effective monitoring systems are set up.
- That relevant procedures in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school e-safety policies and documents (in conjunction with the Designated Safeguarding Lead).
- The Academy's Designated Safeguarding Lead is trained in e-safety issues and is aware of the potential for serious safeguarding issues that could arise through the use of ICT.

Designated Safeguarding Lead

The Designated Safeguarding Lead, supported by the ICT support team, takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, the LA, ICT Technical staff and SLT on all issues related to e-safety and safeguarding;
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Organising training and providing advice for staff;
- Receiving reports of e-safety incidents and ensuring these are recorded on CPOMS to inform future e-safety developments;

Astrea Managed Service

The Astrea Managed Service is responsible for ensuring that:

- The Academy's ICT infrastructure is secure and meets e-safety technical requirements
- The Academy's password policy is adhered to
- The Academy's filtering policy is applied and updated on a regular basis and that its

implementation is not the sole responsibility of any single person

- The use of the Academy's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Designated Safeguarding Lead and/or SLT for investigation/action/sanction.

Teaching & Support Staff

In addition to elements covered in the Staff Acceptable Use Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and of the current Academy e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- E-safety issues are embedded in all aspects of the curriculum and other Academy activities
- Students understand and follow the Academy's e-safety and acceptable use policies
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extracurricular and extended Academy activities
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.

Students (to an age-appropriate level)

- Are responsible for using the Academy ICT systems in accordance with the Student Acceptable Use Policy, which they will be required to sign before being given access to the Academy systems.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of the Academy and realise that the school's e-safety policy also covers their actions out of the Academy, if related to them being a member of the Academy community.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their child/ren understand the need to use the internet/mobile devices in an appropriate way. The Academy will therefore take opportunities to help parents and carers understand these issues.

Parents and Carers will be responsible for:

- Accessing the Academy 's website in accordance with the relevant Academy's Acceptable Usage Policy.
- Monitoring their child's use of devices and the internet when not in the Academy

Education and Training

E-safety education will be provided in the following ways:

- An e-safety programme is provided and is regularly revisited in ICT and other lessons across the curriculum – this covers both the use of ICT and new technologies in and outside the Academy
- Students are taught to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Students are helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of the Academy.
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff act as good role models in their use of ICT, the internet and mobile devices.

Acceptable Use Policy (see Appendix 1 – Students and Appendix 2 – Staff, Volunteers and Visitors)

- **Students** will be required to read through and sign the AUP prior to using devices in the Academy.
- **Staff and regular visitors** to the Academy have an AUP that they must read through and sign to indicate understanding of the rules.

Copyright

- Students will be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Students are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.

Communication

Email

- Digital communications with students (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official Academy systems (see staff guidance in child protection policy).
- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, Academy curriculum systems);
- Under no circumstances should staff contact students, parents/carers or conduct any Academy business using personal e-mail addresses.
- The Academy e-mail is not to be used for personal use. Staff can use their own email in the Academy (before, and after the Academy Day and during lunchtimes when not working with students) – but not for contact with parents/carers/students.

Mobile Phones

- **School mobile phones** only should be used to contact parents/carers/students when on the Academy business with students off site. Staff should not use personal mobile devices unless this is unavoidable, in which case the number must be withheld.
- **Staff** should not use personal mobile phones in the Academy during working hours when in contact with students.
- **Students** should adhere to the Academy rules and guidelines regarding mobile phone use in the Academy (see the Positive Behaviour Management Policy)

Social Networking Sites

Students will not be permitted to access social networking sites at the Academy; at home it is the responsibility of their parent/carer, but parents/carers should be aware that many popular sites have a minimum age of 13.

- **Staff** should not access social networking sites for personal reasons on Academy equipment in school or at home. Staff should access sites using personal equipment.
- **Staff** users should not reveal names of staff, students, parents/carers or any other member of the Academy community on any social networking site or blog**.**
- **Students/Parents/carers** should be aware the Academy will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.
- If inappropriate comments are placed on social networking sites about the Academy the Academy or Academy staff then advice will be sought from the relevant agencies, including the police if necessary.
- Students will be taught about e-safety on social networking sites as we accept some may use these outside of the Academy..

Digital Images

- The Academy record of parental permissions granted/not granted must be adhered to when taking images of our students. All information is stored in the Academy's Information Management System.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Principal or the Designated Safeguarding Lead
- Where permission is granted the images should be transferred to the Academy storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the Academy will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The Academy has an active website, Twitter and Facebook accounts which are used to inform, publicise Academy events and celebrate and share the achievement of students.

Removable Data Storage Devices

- Students should not bring their own removable data storage devices into the Academy unless asked to do so by a member of staff.

Websites

- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger students who may misinterpret information.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents / Carers will be advised to supervise any further research.

Passwords

Staff

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems

Students

- Should keep their passwords secure and not disclose them to other students.
- Should inform staff immediately if passwords are traced or forgotten.
- Ask a member of staff to change their password if they believe the security of their password has been compromised.

Use of Own Equipment

- Privately owned ICT equipment should never be connected to the Academy's network without the specific permission of the Principal or Network Manager.
- Students in Years 7-11 should not bring in their own equipment unless asked to do so by a member of staff. Sixth form students may bring in their own equipment for use in the sixth form block only.

Use of School Equipment

- No personally owned applications or software packages should be installed on to the Academy's ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All should ensure any screens are locked (by pressing Alt, Ctrl & Delete simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

Monitoring

All use of the Academy's internet access is logged and the logs are randomly but regularly monitored by the Academy's IT staff. Whenever any inappropriate use is detected it will be followed up by the Designated Safeguarding Lead, Head of Year or members of the Senior Leadership Team depending on the severity of the incident.

Incident Reporting

Any e-safety incidents must immediately be reported to the Principal (if a member of staff) or the Designated Safeguarding Lead (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

Responding to incidents of misuse

It is hoped that all members of the Academy community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, in most cases this will be reported to the police and any evidence preserved by confiscating a device if necessary. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. Incidents will be dealt with as soon as possible in a proportionate manner, and relevant members of the school community kept informed. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Appendix 1

Longsands Academy Student Acceptable Use Agreement

This document is a guide to young people to be responsible and stay safe while using the Internet and other communication technologies. It clearly states what use of computer resources is acceptable and what is not. Irresponsible use may result in the loss of Internet or computer access, contact with parents/carers or in the event of illegal activities contact with the police.

- I will only access the Academy network through my authorised username and password. I will not use the passwords of others.
- I will not use the Academy ICT systems for personal or recreational use, for on-line gaming, gambling, internet shopping, file sharing or video broadcasting.
- I will not try to upload, download or access any materials which are illegal, inappropriate or which may cause harm and distress to others.
- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place.
- I will not try to install programmes on any Academy computer or try to alter computer settings.
- I will only use my personal hand held devices (e.g. mobile phone/iPod) in the Academy at times that are permitted. This is when commuting to and from school, or to contact parents after 4pm following participation in an extra-curricular activity. Sixth form students may use their own devices, including mobile phones during the day in the Sixth Form block. When using my own devices I understand that I have to follow the rules set out in this document.
- I will carefully write email and other on-line messages making sure the language I use is not strong, aggressive or inappropriate and shows respect for others. I am responsible for the emails I send and the contacts I make.
- I will not open emails unless I know and trust the person/organisation who has sent them.
- For my own safety and that of others, I will not disclose personal information about myself or others when on-line. I will not arrange to meet 'on-line friends' unless I take an adult.
- I will not take, or distribute, images of anyone without their permission.
- I will only use chat and social networking sites with permission and at the times that are allowed.
- I will report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- Where the material I research on the Internet is protected by copyright, I will not try to download copies, including music and video. I will only use the work of others found on the Internet in my own work with their permission.
- I will take care to check that information I find on the Internet is accurate and understand that some work found on the Internet can be untruthful or misleading.
- I will immediately report any damage or faults involving IT equipment, however this may have happened.

Signed ..... Date .....

Appendix 2

Longsands Academy Staff/Volunteer/Visitor Acceptable Use Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside the Academy. The internet and other digital information and communications are powerful tools, which open up new opportunities for everyone. These technologies can inspire discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users have an entitlement to safe Internet access at all times.

This policy is intended to ensure that:

- Staff and volunteers will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- All Longsands Academy ICT systems users are protected from accidental or deliberate misuse that could put the security of the systems or users at risk.
- Staff are protected from potential risk in their use of ICT in their everyday work.

The Academy will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to improve learning opportunities for all and will, in return, expect staff, volunteers and authorised visitors to agree to be responsible users.

Responsible Use Agreement

I understand that I must use Longsands Academy ICT systems in a responsible way to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that learners receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with students.

For my professional and personal safety:

- I understand that the Academy will monitor my use of ICT systems, email and other digital communications.
- I understand the rules set out in this agreement also apply to the use of the Academy ICT systems (e.g. laptops, email, Learning Platform etc.) out of the Academy.
- I understand that the Academy ICT systems are primarily intended for educational use and that I will only use systems for personal or recreational use within the policies and rules set down by the Academy.
- I will not disclose my username and password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material/incident I become aware of to the Designated Safeguarding Lead or member of the Senior Leadership Team.

Signed ..... Date .....