Online Safety Policy

Langley Park School for Boys

Last updated June 2022

1. What is Online Safety

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning, there are still dangers related to their use, especially in relation to young students. Some examples of this are:

- Bullying via chat or email (Cyberbullying)
- Obsessive internet use
- Exposure to inappropriate materials
- Inappropriate or illegal behaviour
- Physical danger of sexual abuse

As a school it is our duty of care alongside that of parents and other members of the community to protect our students from these dangers and this can be achieved by many different mechanisms working together.

The purpose of this online safety policy is to outline what measures the academy takes to ensure that students can work online in a safe environment and that any online safety issue is detected and dealt with in a timely and appropriate manner.

2. Audience

This document is intended for public consumption as well as that of academy members, parents and local community and is a clear outward statement on the academy online safety practices.

3. General policy statement

The academy will endeavour to ensure the online safety of all academy members. It will use education, technology, accountability, responsibility and legislation as the key ways to achieve this.

4. Whole school responsibilities for online safety

Within the academy all members of staff and students are responsible for online safety, responsibilities for each group include:

The online designated safeguarding lead

The school's online designated safeguarding lead (ODSL) is **Ben Jones** [Assistant Headteacher]

The ODSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and organising the delivery of staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

Students

- Participating in and gaining an understanding of online safety issues and the safe responses from online safety training sessions
- Compliance with a highly visible student's Acceptable Use Policy (AUP) which students must agree to each time they use academy ICT equipment either in the academy or remotely which connects to the internet
- Reporting any online safety issues to the teacher, leadership group member or parent
- Take responsibility for their own actions using the internet and communications technologies.

All Staff and volunteers

- Have a clear understanding of online safety issues and the required actions from online safety training sessions
- Reporting any online safety issues to the online safety manager as soon as the issue is detected
- Compliance with a highly visible staff Acceptable Use Policy (AUP) which staff must agree to each time they use the LPSB ICT equipment either in the school or remotely which connects to the internet.

Teaching Staff

- Educating students on online safety through specific online safety training sessions and re-enforcing this training in the day to day use of ICT in the classroom.

Network Manager (CTS)

- Ensure that the best technological solutions are in place to ensure online safety as well as possible whilst still enabling students to use the internet effectively in their learning
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any online safety breach.
- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible
- Works with the online safety Manager to create, review and advise on online safety and acceptable use policies.

Head of Computing

- Leads the development of the online safety education programme for students and staff
- Manages a parental awareness programme for online safety

Online Safety Manager

- Deals with online safety breaches from reporting through to resolution in conjunction with the ICT support team
- Works with the ICT Manager and ICT Director to create, review and advise on online safety and acceptable use policies
- Maintains a log of all online safety issues

ICT Support Team

- Monitors the technology systems which track student internet use to detect online safety breaches
- Assists in the resolution of online safety issues with the online safety manager and other members of staff

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Lee Game [Staff Governor].

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

5. How LPSB ensures Online Safety in the classroom

Educating students in online safety

A clear objective of LPSB is to educate students in safe use of ICT and the internet. LPSB believes this is one of the best ways to minimise the potential for any online safety issues to occur.

- Students will receive specific online safety lessons aimed at ensuring that:
- Students know the online safety risks and how to identify when they are at risk
- Students know how to mitigate against online safety risks by using e-safe practices whilst online
- Students know when, how and to whom to report instances when their online safety may have been compromised
- Students know that they are in an environment that encourages them to report online safety issues without risk of reprimand, humiliation or embarrassment.

LPSB will follow the Think U Know programme by the government's Child Exploitation and Online Protection (CEOP) centre as one of the primary education tools.

In addition to this specific training all members of staff will have a duty to reinforce online safety practices wherever possible and will offer students advice and support in the classroom where minor online safety incidents have occurred.

Online safety education information will have high visibility in all areas of the academy.

Acceptable Use Policies

All members of LPSB – students, staff and parents – must agree to an Acceptable Use Policy (AUP) before they can use the ICT systems at LPSB. With respect to online safety the AUP details:

- The users responsibilities
- Activities which are appropriate and inappropriate
- Best practice guidelines
- How the academy will monitor online safety
- What information is collected

How online safety is monitored

- The ICT support team will actively monitor the students' ICT activity using a monitoring system which can flag potential online safety issues
- The ICT team will periodically review internet access logs to track any websites which could potentially present an online safety issue
- The online safety manager will periodically review the online safety log to track trends and use the information to look at ways of improving the students' online safety
- Teaching staff will directly monitor the students' ICT and internet use in the classroom

How technology is used

LPSB will employ many different technologies to help to ensure online safety for all its members:

- LPSB will use internet filtering to block inappropriate content as designated by the DfE and in addition block websites which are irrelevant to the students' programme of study and are considered time wasting.
- LPSB will use a system which tracks all student activity on the school's computers. This system will automatically flag potential online safety issues which will be monitored and then can be investigated by the support for learning team.
- LPSB will restrict which activities the students can perform using ICT and the internet through systems security policy and access control.
- Teaching staff will use control mechanisms to attempt to limit the applications and web sites which the students can visit whilst using ICT within a lesson.

6. How LPSB will respond to issues of misuse

The following are provided for the purpose of example only. Whenever a student or staff member infringes the online safety policy, the final decision on the level of sanction will be at the discretion of the Headteacher.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the ODSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Students:

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other mobile devices) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

(Possible Sanctions: referral to online safety manager / removal of device until end of day / contact with parent / removal of internet access rights for a period)

Category B infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile device after being warned
- Accidentally accessing offensive material and not notifying a member of staff of it

(Possible Sanctions: referral to Online Safety Manager / Head of Year / removal of device until the end of the week / contact with parent / removal of Internet access rights for an extended period / fixed term exclusion)

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the internet
- Transmission of commercial or advertising material

(Possible Sanctions: referral to online safety manager / Headteacher / contact with parent / removal of equipment / removal of Internet and / or Learning Platform access rights for an extended period / exclusion / referral to police)

Category D Infringements

- Continued sending of emails or social media messages regarded as harassment or of a bullying nature after being warned
- Sending 'youth produced sexual imagery' via email, MMS message or any other social media platforms / applications.
- Having 'youth produced sexual imagery' stored in their account or mobile device.
- Failing to notify a member of staff if they have been sent a 'youth produced sexual image'
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent

- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

(Possible Sanctions: Referral to online safety manager / Headteacher / exclusion / removal of equipment / referral to police / referral to LA online safety officer)

Staff:

Category A Infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging, etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

(Sanction – referral to line manager / Headteacher / Warning given)

Category B Infringements (Gross Misconduct)

- Serious misuse of , or deliberate damage to, any school computer hardware or software
- Any deliberate attempt to breach data protection or computer security rules
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

(Sanction – referral to headteacher and follow the school disciplinary procedures / police / GTC / Governors)

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended, and the school disciplinary procedures implemented.

Other Safeguarding Actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school
- Identify the precise details of the material
- Where appropriate, involve external agencies as part of these investigations

How will staff and students be informed of these procedures?

- Procedures are included within the school's online safety / Acceptable Use Policy. All staff are required to sign the school's online safety policy acceptance form
- Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'. Pupils are required to sign an age appropriate online safety / acceptable use form
- The school's online safety policy will be made available to parents who are required to sign an acceptance form when their child starts at the school
- Staff are issued with the 'What to do if?' guide on Online Safety issues

7. Working with parents and the community

Clearly many academy students will also have access to ICT and the internet at home, often without some of the safeguards that are present within the academy environment. Therefore, parents must often be extra vigilant about their child's online safety at home.

One of the goals of the academy is to support parent's role in providing an e-safe environment for their children to work in outside the academy.

The academy will do this in several ways:

- Run training sessions and workshops on online safety
- Publish online safety information and direct parents to external online safety advisories via the parental portal and the school website

8. Acceptable Use Policies

The academy has the following acceptable use policies in place which must be agreed to before the relevant individuals will be able to access ICT systems and the internet.

- Staff ICT and the Internet Acceptable Use Policy
- Students ICT and the Internet Acceptable Use Policy
- Parents Acceptable Use Policy for Parents Portal Access

A copy of these policies is available on request. The academy will regularly review and update these policies.

9. Safeguarding and remote education during school closure (COVID-19 or similar)

Safeguarding pupils and teachers online

Keeping pupils, students and teachers safe during remote education is essential. Teachers delivering remote education online are aware that the same principles set out in the school or college staff behaviour policy will apply.

All staff will have read the latest KCSIE which includes information and support to help schools keep children and young people safe online.

Important conversations with parents, carers, pupils and students

The importance of a safe online environment will be emphasised to parents, carers, pupils, and students. Which amongst other things, means keeping any log-in credentials and passwords safe.

It is especially important for parents and carers to be aware of what their children are being asked to do, including:

- sites they will be asked to use
- school staff their child will interact with

Reporting concerns

All school staff will continue to act immediately (following the child protection policy and the processes set out in Part 1 of Keeping Children Safe in Education) if they have any concerns about a child or young person's welfare, whether the child or young person is physically in school or learning from home.

Pupils and students are encouraged to speak up if they come across something worrying online.

Communicating with parents, carers, pupils and students

Where education is taking place remotely the school will:

- communicate within school hours as much as possible
- communicate through the school or college channels approved by the senior leadership team
- use school or college email accounts
- use school or college devices over personal devices wherever possible
- advise staff not to share personal information
- ensure parents and carers are clear when and how they can communicate with teachers
- ensure logins and passwords are secure and pupils and students understand that they should not share this information with others

Teachers should try to find a quiet or private room or area to talk to pupils, students, parents or carers. When broadcasting a lesson or making a recording, consider what will be in the background.

Virtual lessons and live streaming

Remote teaching will include both recorded or live direct teaching time, and time for pupils and students to complete tasks and assignments independently.

Where possible the school will:

- use neutral or plain backgrounds

- ensure appropriate privacy settings are in place
- ensure staff understand and know how to set up and apply controls relating to pupil and student interactions, including microphones and cameras
- set up lessons with password protection and ensure passwords are kept securely and not shared
- ensure all staff, pupils, students, parents and carers have a clear understanding of expectations around behaviour and participation