Langley Park Learning Trust

# Online Safety Policy

| | |
|---|---|
| Owner (job role): | Data Protection Officer |
| Approval Body: | Resource and Finance Committee |
| Approval Date: | 10 December 2020 |
| Implementation Date: | 1 January 2021 |
| Review Date: | 1 January 2022 |

| Version | Approval Date | Summary of Changes |
|---|---|---|
| | | |
| | | |

# LPLT ONLINE SAFETY POLICY

## Introduction

Today's pupils are growing up in a world where online and offline life is almost seamless. This offers many opportunities but also creates challenges, risks and threats. At Langley Park Learning Trust we try to equip our pupils with the knowledge to be able to use technology to their best advantage in a safe, considered and respectful way.

The Trust recognises the importance of treating online safety as an ever-present serious safeguarding issue and its teaching as a whole school issue and the responsibility of all staff. It is important to protect and educate both pupils and staff and have supportive mechanisms, policies and protocols in place to protect and support the school community.

Ofsted reviews online safety measures in schools and there are numerous Acts of Parliament which relate when considering the safeguarding of both staff and pupils in schools. The safeguarding aspects of Online safety are evident in all our ICT/safeguarding policies and procedures throughout the school and it is essential that this constantly developing area of technology is kept under review.

It is also critical to ensure the safety and security of all personal data that the school holds and processes. Under the General Data Protection Regulation, the school is responsible for exacting standards of safety and security of personal data that may be processed.

This policy links all the ICT, safeguarding and other policies and procedures to reflect how the school deals with online safety issues on a daily basis.

## Objectives and targets

This policy is aimed at making the use of electronic communication at within our school as safe as possible. This policy applies to all members of the Trust community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to, and are users of, school ICT systems, both in and out of school.

## Action plan

Each school, with support from the network manager/technical support provider, will deal with any online safety incidents which arise by invoking this policy, other ICT policies and the associated behaviour and anti-bullying policies. The school will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school and take appropriate action.

Any breaches of safety of personal data held by the school that may arise will be dealt with as soon as they come to light and the appropriate authorities notified.

The following sections outline:

- The roles and responsibilities for online safety of individuals and groups within the school, and how they will receive education/training to fulfil those roles.
- How the infrastructure is managed.
- How online safety is considered in the curriculum.
- The protocols on using digital images.
- The protocols on data protection.
- The protocols for handling electronic communication.

- Awareness of and dealing with inappropriate use of electronic media.

## Roles and responsibilities – trustees and governors

- Filtering and monitoring is an important part of the online safety and governors ensure that appropriate filters and monitoring systems are in place on the school's ICT resources. Moreover, the trustees and governors oversee a whole school approach to online safety, which includes policies and procedures on mobile technology use in the school. Some pupils have access to the internet via 3G or 4G enabled devices unfiltered by the school and the school's policy on confiscation of inappropriate items will be used if it is found that such devices are being used inappropriately on the premises.

- Trustees and governors will ensure compliance with the Data Protection Act and the GDPR for all personal data held.

- Trustees and governors will ensure that pupils are taught about online safety, for example through personal, social, health and economic education (PSHE) and through relationships education (primary schools) and relationships and sex education (RSE) (secondary schools).

- Trustees and governors are responsible for the approval of the online safety policy, for reviewing the effectiveness of the policy and for dealing with issues when they arise.

- A nominated link governor for online safety is appointed as a member of the school's online safety committee.

- Governors receive Online safety training/awareness sessions as part of their annual cycle of training.

## Roles and responsibilities – headteacher and senior leaders

- The headteacher is responsible for ensuring the online safety of members of the school community and will manage the education of pupils and training of staff in Online safety and awareness of potential radicalisation in pupils.

- The headteacher, together with the Trust's data protection officer, is responsible on a day-to-day basis for ensuring compliance with the Data Protection Act and GDPR for the processing of personal data.

- The headteacher and another member of the senior leadership team/online safety co-ordinator will be aware of the procedures to be followed in the event of a serious Online safety allegation being made against a member of staff, including the headteacher.

- The headteacher will take appropriate action if it is felt that any pupil of the school may be becoming radicalised.

- The Education and Inspections Act 2006 empowers the headteacher, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying, or other online safety incidents covered by this policy, even though they may take place out of school, but are linked to membership of the school.

## Roles and responsibilities – school Online safety co-ordinator

The school's Online safety co-ordinator:

- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policy and other related policies, including the safe processing of personal data.
- Ensures that all members of staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff to ensure that all teaching is carried out in an age-appropriate way.
- Reports to the headteacher any suspicions of pupils who may be becoming radicalised.
- Liaises with school ICT technical staff.
- Reports regularly to the senior leadership team/headteacher.
- Will receive training at regular update sessions and by reviewing national and local guidance documents.

## Roles and responsibilities – IT support service manager / network manager

The network manager is responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- That appropriate filters and monitoring systems are in place.
- That the school meets the online safety technical requirements outlined in the relevant national/local ICT security policy and/or acceptable usage/Online safety policy and guidance.
- Users may only access the school's networks through a properly enforced password protection policy.
- The headteacher is informed of any suspicions of pupils who may be becoming radicalised.
- The headteacher is informed of any breaches in the processing of personal data.
- The network manager/technical support provider will receive appropriate training on a regular basis from approved trainers to support the online safety of all members of the school community.

## Roles and responsibilities – teaching and support staff

Teaching and support colleagues are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy.
- They have read, understood and signed the relevant staff acceptable computer usage agreement and staff laptop usage agreement, as well as other related policies eg staff e-mail, social media, use of personally owned ICT devices and professional identity protection.
- They report any suspected misuse or problem to the online safety co-ordinator/headteacher/senior leader/head of ICT/ICT co-ordinator/class teacher/head of year as appropriate for investigation/action/sanction.
- They report any suspected breach of processing any personal data to the online safety co-ordinator/headteacher/senior leader/ network manager/technical support provider.
- Digital communications with pupils (email/virtual learning environment (VLE)/voice) are on a professional level and only carried out using official school systems.
- Pupils understand and follow the school online safety policy and the pupil acceptable computer usage policy.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They monitor ICT activity in lessons and in extracurricular and extended school activities.
- They are aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- They are aware of the online safety issues pertaining to email and social media usage.
- They are alert to, and report to the headteacher, any suspicions of pupils who may be becoming radicalised.
- In lessons where internet use is pre-planned, pupils 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.
- All staff receive online safety training and understand their responsibilities, as outlined in this policy. An audit of the Online safety training needs of all staff will be carried out regularly. Training will be offered as a planned programme of formal online safety training available to all staff. All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online safety policy and acceptable usage policies.

### Roles and responsibilities – designated safeguarding lead

The designated safeguarding lead is trained in online safety issues and will be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data.

- Access to illegal/inappropriate materials.
- Inappropriate online contact with adults/strangers.
- Potential or actual incidents of grooming.
- Online bullying.
- Sexting.
- Suspicions of radicalisation.

## Roles and responsibilities – pupils

The rules for use of ICT systems/internet will be posted in all relevant rooms and displayed on log-on screens so that pupils are aware of their responsibilities.

Pupils:

- Are responsible for using the school ICT systems in accordance with the pupil Acceptable Use policy and agreement, which will be introduced to pupils when they first use ICT and then regularly reiterated. Pupils will also be remined of key aspects of acceptable use and Online safety via an online message each time they log in.

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials, including suspicions of pupils who may be becoming radicalised, and know how to report such abuse.

- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- Will be expected to know and understand school rules on the use of mobile phones, digital cameras and hand-held devices, including the school's policy on confiscation of inappropriate items where it relates to the use of mobile phones.

- Will be expected to understand the key principles of the Your Own Device policy as appropriate.

- Will be expected to know and understand the dangers of social networking sites as well as their benefits.

- Will understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety policy covers their actions out of school.

## Roles and responsibilities – parents/carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

- Parents and carers will be responsible for endorsing (by signature) the pupil acceptable computer usage agreement.

Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through:

- Sending information on internet safety and the importance of monitoring internet use at home to all parents annually.
- Parents' evenings.
- Newsletters.
- Letters.
- Website/VLE.
- Information about all relevant national/local Online safety campaigns/literature.
- Information about useful organisations /support services for reporting Online safety issues.

## Online safety in the curriculum

Online safety is taught in specific areas of the curriculum but is also emphasised whenever pupils are using computers online. Staff always consider age-appropriateness when speaking of Online safety and will be aware of those pupils who may be particularly vulnerable, eg looked-after children or those with special needs. The school may use external resources and external visitors to assist in lessons, but appropriate members of staff will check in advance to ensure that they will enhance lessons and that materials used are appropriate for them.

## Relationships education or relationships and sex education

Pupils are taught about:

- Online safety and harm.
- Positive, healthy and respectful relationships online.
- The effects of their online actions.
- How to recognise and show respectful behaviour online.

## Computing in the curriculum

- Principles of online safety.
- Where to obtain help and support if they are concerned about any online content or contact.

## Citizenship in the curriculum

- Media literacy online.
- Distinguishing fact from fiction online.

## Online safety throughout the curriculum

Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities, including:

- How to evaluate what they see online – to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.

- How to recognise persuasion techniques.

- How to recognise acceptable and unacceptable online behaviour – to understand the need for the acceptable computer usage agreement and to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

- How to identify online risks.
- How and when to seek support.
- The need to acknowledge the source of any information used and to respect copyright when using material accessed on the internet.

In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.

Where pupils are allowed to search the internet freely, eg. using search engines, staff are vigilant in monitoring the content of the websites the pupils visit.

It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics (eg. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network manager temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need.

## Management of infrastructure

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed in ways that ensure that the school meets the online safety technical requirements outlined in the acceptable computer usage policy and any relevant LA online safety policy and guidance.
- Personal data is held and processed in compliance with the Data Protection Act and GDPR. Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. (See the internal data security policy and e-mail policy.)
- There will be regular reviews and audits of the safety and security of school ICT systems.
- Servers, wireless systems and cabling will be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and will be reviewed, at least annually, by the online safety committee (or other group).
- All users will be provided with a username and password by the network manager.
- The 'master/administrator' passwords for the school ICT system, used by the network manager (or other person) are also available to the headteacher or other nominated senior leader if required and kept in a secure place (eg. school safe).

- Users are made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

- The school maintains and supports the managed filtering service provided by Smoothwall.

- Any filtering issues should be reported immediately to the network manager.

- Pupils are reminded to not download Virtual Personal Networks (VPNs)

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the acceptable computer usage policy.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users.

- Agreements are signed by members of staff in possession of school-provided laptops regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other personally owned devices that may be used out of school.

- The school infrastructure and individual workstations are protected by up-to-date virus software.

## Protocols on using digital and video images

- When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet eg on social networking sites.

- If any incidents come to light about 'sexting' ie the sharing of sexual images of pupils under 18, the designated safeguarding lead should be advised in the first instance.

- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

- Any images should only be taken on school equipment. Personal equipment of staff should not be used for such purposes.

- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Written permission from parents or carers will be obtained.

## Protocols on home-based virtual learning

- Where teachers are delivering lessons remotely, staff and pupils must use an approved system such as MS Teams.

- Pupils are not to use webcams. Where possible, school systems must block pupils' ability to activate webcams during lessons.

- Pupils should be reminded to not record or video live lessons where teachers are using webcams.

## Protocols on data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act and in compliance with the General Data Protection Regulation which state that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Kept no longer than is necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Only transferred to others with adequate protection.

Staff will ensure that they comply with the internal data security policy by:

- Taking care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Using personal data only on secure password protected computers and other devices, and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data.

- Transferring data using encryption and secure password protected devices.

## Protocols for handling electronic communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.

- Users need to be aware that email communications may be monitored.

- Users will be expected to know and understand school policies on email, social media (and other relevant electronic devices protocols.)

- Users must immediately report, to the nominated person, in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy.

- Any digital communication between staff and pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content.

## Unsuitable/inappropriate activities

Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in a school context and users must not engage in these activities in school or outside school when using school equipment or systems. The school policies on child protection, safeguarding and online safety must be followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity eg:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Potential radicalisation of pupils.

Should any serious online safety incidents take place, the appropriate external authorities will be informed eg local area designated safeguarding officer, police etc or, for personal data breaches, the Information Commissioner's Office (ICO).

## Monitoring and reviewing

The school will monitor the impact of the policy using:

- Logs of reported incidents.

- Monitoring logs of internet activity (ie ISP, school network or managed service as appropriate).

- Internal monitoring data for network activity.

The policy will be reviewed by Trustees annually, or more regularly, in the light of any new legislation, any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to online safety as advised by the online safety committee or others. .