



Addison Gardens
Blythe Road
London W14 0DT

Addison Primary School



E Safety Policy

Approved

Summer 2024



1. The main areas of risk for our school community can be summarised as follows:

1.1 Content

- 1.1.1 Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- 1.1.2 Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- 1.1.3 Hate sites
- 1.1.4 Content validation: how to check authenticity and accuracy of online content

1.2 Contact

- 1.2.1 Grooming
- 1.2.2 Online bullying in all forms
- 1.2.3 Identity theft (including 'frape' (hacking Facebook profiles, Instagram, etc...)) and sharing passwords

1.3 Conduct

- 1.3.1 Privacy issues, including disclosure of personal information
- 1.3.2 Digital footprint and online reputation
- 1.3.3 Health and well-being (amount of time spent online (Internet or gaming))
- 1.3.4 Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- 1.3.5 Extremism
- 1.3.6 Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Role	Key Responsibilities
A. Head	1 To take overall responsibility for Online Safety provision
Teacher /	2 To take overall responsibility for data and data security
Deputy	3 To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL
Head	4 To be responsible for ensuring that staff receive suitable training to carry out their Online safety roles and to train other colleagues, as relevant
Teacher	5 To be aware of procedures to be followed in the event of a serious e-safety incident
	6 To receive regular monitoring reports from the Online Safety Coordinator / Officer/ technician
	7 To ensure that there is a system in place to monitor and support staff who carry out internal Online safety procedures e.g. network manager



Role	Key Responsibilities
<p>B. IT Coordinator / Designated Child Protection Lead</p>	<ol style="list-style-type: none"> 1 Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents 2 Promotes an awareness and commitment to Online safeguarding throughout the school community 3 Ensures that Online safety education is embedded across the curriculum 4 Liaises with school Computing technical staff 5 To communicate regularly with SLT and the designated Online Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs 6 To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident 7 To ensure that an Online safety incident log is kept up to date 8 Facilitates training and advice for all staff 9 Liaises with the Local Authority and relevant agencies 10 Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> • sharing of personal data • access to illegal / inappropriate materials • inappropriate on-line contact with adults / strangers • potential or actual incidents of grooming • Online bullying and use of social media
<p>C. Governors / Child Protection Governor</p>	<ol style="list-style-type: none"> 1 To ensure that the school follows all current Online safety advice to keep the children and staff safe 2 To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor 3 To support the school in encouraging parents and the wider community to become engaged in e-safety activities 4 The role of the Online Safety Governor will include: 5 Regular review with the Online Safety Coordinator / Officer 6 Online safety incident logs, filtering / change control logs
<p>D. IT Coordinator</p>	<ol style="list-style-type: none"> 1 To oversee the delivery of the online safety element of the Computing curriculum 2 To liaise with the online safety coordinator regularly



Role	Key Responsibilities
E. Network Manager/ technician	<ol style="list-style-type: none"> 1 To report any online safety related issues that arise, to the Online safety coordinator. 2 To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed 3 To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) 4 To ensure the security of the school IT system 5 To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices: <ul style="list-style-type: none"> • the school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • that he / she keeps up to date with the school's Online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • that the use of the <i>network/ remote access / email</i> is regularly monitored in order that any misuse / attempted misuse can be reported to the <i>Online Safety Coordinator / Officer / Head Teacher for investigation / action / sanction</i> 6 To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster 7 To keep up-to-date documentation of the school's online security and technical procedures
F. LGfL Nominated contact(s)	<ol style="list-style-type: none"> 1 To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
G. Teachers	<ol style="list-style-type: none"> 1 To embed online safety issues in all aspects of the curriculum and other school activities 2 To supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant) 3 To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role	Key Responsibilities
H. All staff	<ol style="list-style-type: none"> 1 To read, understand and help promote the school's e-safety policies and guidance 2 To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy 3 To be 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 4 To report any suspected misuse or problem to the online safety coordinator 5 To maintain an awareness of current online safety issues and guidance e.g. through CPD 6 To model safe, responsible and professional behaviours in their own use of technology 7 To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
I. Pupils	<ol style="list-style-type: none"> 1. Read, understand and adhere to the Student / Pupil Acceptable Use Policy 2. Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations 3. To understand the importance of reporting abuse, misuse or access to inappropriate materials 4. To know what action to take if they or someone they know feels worried or vulnerable when using online technology 5. To know and understand school policy on the use of mobile phones, digital cameras and hand held devices 6. To know and understand school policy on the taking / use of images and on cyber-bullying 7. To 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, if related to their membership of the school 8. To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home 9. to help the school in the creation/ review of e-safety policies
J. PTA Lead	<ol style="list-style-type: none"> 1. Educating Parents and raising awareness as instructed by Head / IT Co-ordinator



Role	Key Responsibilities
K. Parents/ carers	<ol style="list-style-type: none">1. To support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images2. To read, understand and promote the school Pupil Acceptable Use Agreement with their children3. To access the school website / DB PRIMARY / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement.4. To consult with the school if they have any concerns about their children's use of technology
L. External groups	<ol style="list-style-type: none">1. Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

2 Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: (Poster Making, Drama, Write blogs, videos, music).

2.1 A planned e-safety curriculum should be provided as part of Computing, PHSE (Literacy and foundation subjects where necessary) and should be regularly revisited.

2.2 Key e-safety messages should be reinforced as part of a planned program of assemblies and pastoral activities.

2.3 Pupils should be taught in all lessons to be critically aware of the materials or content they access on-line and be guided to validate the accuracy of information.

2.4 Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

2.5 Staff will act as good role models in their use of digital technologies on the internet and mobile devices.



2.6 In lessons where internet use is pre-planned, it is expected that 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.

2.7 Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

2.8 It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination, sex education (science) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

3 Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

3.1 Curriculum activities

3.2 Parents Meetings

3.3 Parent Workshops

3.4 Newsletter messages

3.5 School Website

4 Staff and governor training This school:

4.3 Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;

4.4 Makes regular training available to staff on online safety issues and the school's online safety education programme.

4.5 Provides, as part of the induction process, all new staff (including those on university/college placement and work experience) with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

5 Other policies to read in conjunction with this document include:

5.3 Sexual harassment and sexual abuse

5.4 Behaviour and discipline

Updated: Summer 2024

Next review: Summer 2026