



Online Safety Policy

Introduction

National guidance suggests that it is essential for schools to take a leading role in Online Safety.

The Byron Review “Safer Children in a Digital World” stressed the role of schools:

“One of the strongest messages I have received during my review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to government in the following areas: delivering Online Safety through the curriculum, providing teachers and the wider children’s workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area.”

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. Schools have made a significant investment both financially and physically to ensure these technologies are available to learners. The benefits are perceived to “outweigh the risks.” However, schools must, through their Online Safety policy, ensure that they meet their statutory obligations to ensure that children and young people are safe and are protected from potential harm, both within and outside school.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Earlsdon’s Online Safety Policy operates in conjunction with our policies relating to student behaviour and discipline, acceptable use, anti-bullying, curriculum, data protection and safeguarding and child protection.

We are committed to making sure that the whole school community is fully involved in the issue of Online Safety. We are actively committed to making sure governors, all adults working in school, our parents and our pupils are provided with up-to-date information, guidance and strategies relating to Online Safety on our school website, twitter feed and weekly newsletter. We are also committed to ensuring that children are taught to recognise when they are at risk, and how to get help if they need it.

As with all other risks, it is impossible for our school to eliminate the risks related to ICT completely. It is therefore essential, through good educational provision, to build pupils' resilience of the risks to which they may be exposed, so that they have the confidence and skills to face them and deal with them appropriately.

Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school relating to Online Safety:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governors receiving regular information about Online Safety and related incidents. A member of the governing body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- Meetings with the Headteacher and / or Computing Subject Leader
- Reviewing this policy on an annual basis
- Ensuring their own knowledge of online safety issues is up to date
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals
- Ensuring that there are appropriate filtering and monitoring systems in place
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.

Headteacher(DSL)and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community
- The Headteacher and other senior leaders are responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their Online Safety roles - and to train other colleagues

- The Headteacher and other senior leaders will ensure that there is a system in place to allow for the effective monitoring of internet use
- The Headteacher and other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented
- Ensuring safeguarding is considered in the school's approach to remote learning
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether referrals have been made.
- Understanding the purpose of record keeping
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.

Designated Person for Child Protection

Should be trained in Online Safety issues and be aware of the potential for child protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Incidents of grooming
- Cyber-bullying.

Teaching and Support Staff

Are responsible for ensuring that:

- They have awareness of Online Safety matters and the current school Online Safety policy
- They have read, understood and signed the school staff Acceptable Use Policy
- They report any suspected ICT misuse to the Headteacher in a timely manner
- Digital communications with pupils are kept entirely professional
- Online Safety issues are embedded within the curriculum and other school activities

- Pupils understand and follow the school Online Safety Policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They understand their responsibilities relating to their personal use of social media
- They are aware that any incidents relating to cyber-bullying or Online Safety that occur out of school, will be acted upon by the school
- In the event of being made aware of a 'sharing of nudes and semi-nudes' type incident (formerly known as 'sexting'), they inform a Designated Safeguard Lead of the incident in a timely manner, record relevant details on CPOMS
- They are aware of Online Safety issues related to the use of mobile phones, wearable technologies, cameras and handheld devices, and that they monitor their use and implement current school policies regarding these devices.

Pupils:

- Will understand that incidents relating to cyber-bullying and/or Online Safety that occur out of school, will be investigated and acted upon in school
- Pupils will be educated about the benefits and the risks associated with social media, and will be taught strategies to remain safe when online or accessing social media
- Will be taught to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know school protocol on the use of mobile phones, digital and handheld devices. They should also know and understand school protocol on the taking / use of images, and on cyber-bullying
- Will not use their personal mobile phones/devices on the school site and must hand in any such technology to their class teacher by 9.00am each morning for safe keeping
- Should 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. Pupils will be given their own passwords, and this will be their only means of accessing school computer systems and the internet. They will be taught the importance of password security and will keep their personal password private.

Parents / Carers

Parents / carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Research shows that parents and carers are often less experienced in the use of ICT than their children. The school will therefore take every

opportunity to help parents understand relevant issues through parents' evenings, newsletters, letters, the school website, and by providing information about national or local Online Safety campaigns and/or literature.

The Headteacher will ensure that the school's newsletter will indicate to parents where policies and advice relating to Online Safety are being added to or amended where appropriate. In this way parents can request paper copies if they have limited access to technology at home.

Our school actively encourages parent/carers to contact our school to discuss any Online Safety issues or concerns with the Headteacher or class teacher.

Use of Social Media

Social media websites are being used increasingly to fuel campaigns and complaints against schools, Headteachers, school staff, parents and pupils. Earlsdon Primary School considers the use of social media websites in this way as unacceptable, and not in the best interests of the children or the whole school community. Any concerns must be made through the appropriate channels by speaking to the Class Teacher, the Headteacher or the Chair of Governors, so that they can be dealt with fairly, appropriately and effectively. The school's complaints procedure is available online, via the school website.

In the event that any pupil or parent/carer of a child being educated at Earlsdon is found to be posting libellous or defamatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site. All social network sites have clear rules about the content which can be posted on the site, and they provide robust mechanisms to report content or activity which breaches this. The school will also expect that any parent/carer or pupil removes such comments immediately. In serious cases the school will also consider its legal options to deal with any such misuse of social networking and other sites.

Additionally, and perhaps more importantly, is the issue of cyber bullying. In the event of any member of the school community using social media to publicly humiliate another by inappropriate social network entry, we will deal with this as a serious incident of bullying.

Online Safety – Preventing Radicalisation

The internet provides children and young people with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering systems used in our school blocks inappropriate content, including extremist content. Where staff, children or visitors find unblocked extremist content, they must report it to a member of the Safeguarding Team or School Leadership Team immediately. Pupils and staff should know how to report internet content that is inappropriate or of concern. Children must be given online safety education each year and have regular reminders of the use of CEOPs and online safety links on the school website.

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach when using ICT. The education of pupils in

Online Safety at Earlsdon is therefore a vital part of the school's ICT provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience, and Online Safety education will be provided in the following ways:

- A planned and age-appropriate Online Safety scheme of work (Project Evolve) will be provided for each year group and must be taught annually; this is to be delivered alongside other opportunities including Safer Internet Week and as part of our embedded curriculum where appropriate
- Pupils will be taught about the benefits and the risks associated with social media, and will be taught strategies to remain safe when online or accessing social media
- The school will participate in Safer Internet Day which is organised nationally on an annual basis. These days also serve to refresh, update and remind pupils of the issues that they face every day of the year
- Pupils will be taught across all subjects to be critically aware of the materials / content that they access online, and be guided to validate the accuracy of information
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed via the internet
- Pupils will be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for the use of ICT systems / internet will be shared prior to children logging onto school systems
- Staff will act as good role models in their use of ICT, the internet and mobile devices

Education –Parents / Carers

Many parents and carers have a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and can often be unsure about what they should do about it.

The school will, therefore, seek to provide information and pass on awareness to parents and carers through letters, the school newsletter and the school website.

Education & Training –Staff

It is essential that all adults working with children at Earlsdon receive necessary Online Safety training and understand their responsibilities, as outlined in this policy. In addition, the school will implement a cyber awareness plan for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cyber-crime. The school will implement its cyber security strategy in line with the DfE's 'Cyber security standards for schools and colleges'. The DSL will ensure that all safeguarding training given to staff includes elements

of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life. Training will be offered as follows:

- All new staff with network access should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy
- Online Safety training / CPD will be made available to staff as and when necessary
- Staff will be given training to help them understand the issues of radicalisation and are able to recognise the signs of vulnerability or radicalisation and know how to refer their concerns. This information also forms part of induction safeguarding training.
- This Online Safety policy will be shared with staff
- Members of the Senior Leadership Team will provide advice / guidance / training as required to individuals.

Training –Governors

Governors should take part in Online Safety training / awareness sessions, with this being particularly important for those who are involved in ICT / Online Safety / health and safety / child protection. This may be offered in a number of ways, including attendance at training provided by the Local Authority, National Governors Association or other relevant organisation and participation in school-based training / information sessions for staff or parents.

Technical –Infrastructure / Equipment, Filtering and Monitoring

The school is 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. It will also ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities:

- All users will have clearly defined access rights to school ICT systems
- All users will be provided with a username and password for the school network. This includes teachers, teaching assistants, other designated staff and all pupils in key stages 1 and 2.
- The school is currently using a filtering service provided by Impero. This blocks any sites containing banned words or which come under predetermined categories. Any attempts to access such sites, or the typing of unacceptable words, triggers a screen shot which is sent to a central log. These are then checked Headteacher and Deputy Head.
- Requests from staff for websites to be removed from the filtered list will be considered by the Computing subject leader and members of the SLT. The removal, if approved, will be completed by the school IT support staff
- The Headteacher can monitor the activity of users on the school ICT systems, and users are made aware of this

- Staff are forbidden from installing programmes on school workstations / portable devices without permission from the Headteacher (any such installation requires administrator login)
- The school infrastructure and individual workstations are protected by up-to-date virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Our Earlsdon Curriculum

Online Safety should be a focus in all areas of the curriculum, and all staff should reinforce Online Safety messages in the use of ICT across the curriculum:

- Where pupils are allowed to freely search the internet (e.g. when using search engines) staff should be vigilant in monitoring the content of the websites that young people visit
- Pupils should be made aware that their activities when using school systems can be monitored and recorded, and encouraged / taught to act responsibly when using ICT
- Pupils should be taught by all staff in all salient lessons to be critically aware of the materials / content that they access online and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

Consent and Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing / posting digital images on the internet.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet (such as on social networking sites)
- 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
- Staff will not publish any digital images of themselves, or any other staff engaged in school activities on the personal pages of social networking sites
- Staff will not publish any digital images of pupils engaged in school activities on the personal pages of social networking sites
- Staff will ensure that their personal networking use is restricted, so that it is not publicly available
- Staff will always ensure that their use of social media remains professional and does not bring the school into disrepute. This includes, but is not exclusive to, ensuring that pupils of the

school do not have access to their personal sites unless there are good personal reasons that the Headteacher is aware of

- Care should be taken when taking digital / video images of pupils, to ensure that they are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of other pupils or staff without their permission
- Photographs published on the website, X, 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 must be obtained before photographs of pupils are published on the school website or X account. Staff must be aware of this and not publish images of pupils online where permission has been denied.

Guidance for Using Virtual / Video Conferencing

Video conferencing platforms can be an invaluable tool. However, all staff must be aware that a heightened sense of urgency can also lead to an increased risk regarding safeguarding and data protection. The following section is designed to make explicit the expectations in place when using virtual conferencing and online learning platforms.

- As a school, we Microsoft Teams which can be used for setting homework and is ready for use for home schooling if needed in the future.
- During a lockdown situation, Microsoft Teams meetings can be used to host live sessions with classes and groups of children to maintain effective communication and wellbeing.
- All Microsoft teams meetings with children must be approved by the Designated Safeguarding Lead.
- Microsoft Teams meetings, between class teachers and parents, are used at the start of each school year and are set up by an administrator from the school office.

If the need to work remotely arises, we will consider the following safeguarding issues:

- It is not appropriate for staff members to hold one-to-one video conferences with a pupil/student. The staff Code of Conduct sets out expectations for behaviour.
- Two members of staff should be present for video calls. This is to safeguard pupils/students and members of staff. When meetings are set up for groups of children, one member of staff can host the meeting. Settings to ensure pupils joining a meeting are kept in the lobby to avoid 1-1 interaction.
- Parents/carers must be notified about the use of video conferencing.
- Video conferencing is to be used by adults working with groups of children. Where concerns arise, these should be flagged immediately using CPOMS as per safeguarding policy.
- School safeguarding policies must be adhered to in the event of a child seeking to make a disclosure or remote abuse.

- Pupils/students should be reminded of reporting routes and how to seek help if they need to.
- Staff should separate their remote learning account from their personal online profiles and use a duplicate of the staff notice image or school logo for the platform profile picture. You should set up school accounts for any online platforms you use and check the privacy settings.
- When making telephone calls to parents/carers, either the school landline number or the dedicated school mobile telephone should be used for the purpose of communications.
- Never share any personal information e.g. personal telephone number, email accounts, Facebook and other social media links.
- In the event of video conferencing, staff members are to work against a neutral background. Staff should present themselves as they would if they were giving a face-to-face lesson, in dress and in manner.
- Where lessons are delivered to a class, parents/carers and pupils should be provided with safeguarding and etiquette guidance in advance of the lesson. For example, the pupil/student must take lessons in a room with an open door. Parents should be notified of the timetable for their child in advance of the lessons taking place.
- All staff members can contact the Designated Safeguarding Lead (DSL) or, in the event of the DSL being unavailable, deputy DSL, should they have any concerns about a child. Examples of potential concerns may include a staff member seeing, or hearing, something of concern during communication with a student or a disclosure, made by a pupil/student.
- When making contact directly with pupils/students, as a means of checking on their welfare, schools should consider which methods are most appropriate for each pupil/student.
- Contact with pupils/students should happen within normal school hours.
- Schools should not record online lessons which include pupils without parental permission, or student permission where they have competency to consent.

Data Protection and GDPR

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states 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.

The act states: Under the regulations, it's essential that the data you hold is '**processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures**'.

Staff must ensure that:

- They take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- They use personal / sensitive data only on secure password protected computers and other devices
- Personal / sensitive data is only moved or transported using secure encrypted memory sticks
- They do not store personal or sensitive data on any non-encrypted USB stick or other device.

Escalating Security Incidents e.g. remote hack, password breach

In the event of a security breach the following protocol must be adhered to:

- Report immediately to the Headteacher, on-site technician or SLT
- Isolate and quarantine affected machine(s) – support from technician both on-site and offsite via the IT helpdesk
- Isolate and quarantine affected machine(s) – support from technician both on-site and offsite via the IT helpdesk.

Responding to Incidents of Misuse

It is expected that all members of the school 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 misuse of ICT. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images
- Criminally racist material
- Criminal conduct, activity or materials

The Headteacher must be consulted with the evidence of the activity. If the evidence confirms the misuse the Headteacher has a duty to report the incident to the police.

As per safeguarding guidance – staff should not view images or videos on pupil's personal devices.

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. The investigation should be conducted by the Headteacher or another member of the SLT.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

To be ratified: February 2025