# Roles and responsibilities

|  |  |
| --- | --- |
| Role | Key responsibilities |
| Head teacher | * takes overall responsibility for online safety provision
* take overall responsibility for data and data security (SIRO)
* to ensure the school uses an approved, filtered Internet Service, which adheres to best practice and recommendations
* to be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant
* to be aware of procedures to be followed in the event of a serious online safety incident.
* to receive regular monitoring reports from the Online SafetyCo-ordinator
* 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 or IT support company)
 |
| Online Safety Co-ordinator / Designated Safeguarding Lead | * takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
* promotes an awareness and commitment to e-safeguarding throughout the school community
* ensures that online safety education is embedded across the curriculum
* liaises with school ICT technical staff
* To communicate regularly with SLT and the designated e-safety Governor / committee to discuss current issues, review incident logs and filtering, and school’s change control processes and requests
* To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
* To ensure that an online safety incident log is kept up to date
* facilitates training and advice for all staff
* liaises with the Local Authority and relevant agencies, including making appropriate referrals to Children’s Social Care and/or the police when necessary
* Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
* 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
* extremism and radicalisation
 |
| Governors | * To ensure that the school follows all current online safety advice to keep the children and staff safe
* To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor
* To support the school in encouraging parents and the wider community to become engaged in e-safety activities
* The role of the E-Safety Governor will include:
	+ regular review with the E-Safety Co-ordinator / Officer (including: e-safety incident logs, filtering / change control logs )
 |
| Computing curriculum leader | * To oversee the delivery of the e-safety element of the Computing curriculum
* To liaise with the e-safety coordinator regularly
 |
| Network Manager / Technician | * To report any e-safety related issues that arise, to the e-safety coordinator.
* 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
* To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up to date
* To ensure the security of the school ICT system
* To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices
* 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 e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
* that the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Officer /Headteacher for investigation / action / sanction
* To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a critical incident or system failure
* To keep up-to-date documentation of the school’s e-security and technical procedures
 |
| Data Manager | * To ensure that all data held on pupils on the school office machines have appropriate access controls in place
 |
| Teachers | * To embed e-safety issues in all aspects of the curriculum and other school activities
* To supervise and guide pupils carefully when engaged in learning activities involving online technology ( including, extra-curricular and extended school activities if relevant)
* 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
 |
| All staff | * To read, understand and help promote the school’s e-safety policies and guidance
* To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy
* To be aware of e-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
* To report any suspected misuse or problem to the e-safety coordinator
* To maintain an awareness of current e-safety issues and guidance e.g. through CPD
* To model safe, responsible and professional behaviours in their own use of technology
* 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, social networking sites, etc.
 |
| Pupils (may not all be relevant to EYFS) | * Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at EYFS and KS1 it would be expected that parents / carers would sign on behalf of the pupils)
* to understand the importance of reporting abuse, misuse or access to inappropriate materials
* to know what action to take if they or someone they know feels worried or vulnerable when using online technology.
* have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* to know and understand school policy on the use of mobile phones, digital cameras and hand held devices.
* To know and understand school policy on the taking / use of images and on cyber-bullying.
* To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school’s E-Safety Policy covers their actions out of school, if related to their membership of the school
* To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
* to help the school in the creation/ review of e-safety policies
 |
| Parents/carers | * to support the school in promoting e-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 images
* to read, understand and promote the school Pupil Acceptable Use Agreement with their children
* to access the school website / on-line pupil records in accordance with the relevant school Acceptable Use Agreement.
* to consult with the school if they have any concerns about their children’s use of technology
 |
| External group | * Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school
 |