# HIGH STREET PRIMARY SCHOOL

# E-SAFETY POLICY

# 1. POLICY STATEMENT

New technologies have become integral to the lives of employees and learners in today's society, both within the school and in their lives outside the Academy.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps the school employees and learners learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Learners should have an entitlement to safe internet access at all times.

The requirement to ensure that all people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the school are bound. This is also reflected in the Byron Review, which identified that alongside new technology a new culture of responsibility was needed, where all in society focus not on defending well-established positions, but on working together to help young people keep themselves safe, to help parents/guardians to keep them safe and to help each other support young people and parents/guardians in this task.

# 2. DEFINITIONS

E-Safety is defined as the awareness, practice and training of individuals together with IT infrastructure security and integrity to ensure the safe use of online technologies, thus maintaining both an individual's physical and psychological wellbeing as well as organisational reputation.

# 3. PRINCIPLES

This policy, procedure and guidelines have been produced as a framework for the protection of all in relation to e-Safety.

The education of learners in e-Safety is an essential part of the school's E-Safety provision. Learners need the help and support of the school to recognise and avoid e-Safety risks and build their resilience.

E-Safety awareness will be provided by the school in a variety of ways including; curriculum provision, themed assemblies, an identified e-safety week and through external trainers who will support the work of the school.

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 dependents and in the monitoring/regulation of their on-line experiences. Resources and advice will be made available and shared with parents and carers.

# 4. SCOPE AND LIMITATIONS

This policy applies to all employees, learners, and visitors to High Street Primary School who have access to and are users of the school ICT systems, both in and out of the school.

# 5. RESPONSIBILITIES

The IT Coordinator and the school IT Technician are responsible for ensuring that suitable software and filtering systems are in place, and the whole staff are responsible for overseeing the implementation of this Policy.

# 6. IMPLEMENTATION ARRANGEMENTS

The roles and responsibilities of staff in implementation of this policy and procedures are set out clearly in the procedure.
All new members of staff are made aware of the policy and procedures during the formal staff induction process. Updated and amended procedures will be disseminated and reinforced in training sessions, team meetings and via email communications.
Staff and learners have access to this policy on the school server.

# 7. MONITORING AND REVIEW

The IT Coordinator will be responsible for monitoring the effectiveness of the policy.
Any serious weakness will be reported to the Headteacher, who is the lead professional for child protection.
Due to the ever changing nature of Information and Communication Technologies, the e-Safety Policy will be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of the technologies, new threats to e-Safety, organisational or management changes or incidents that have taken place.

# 8. SUPPORTING AND RELATED DOCUMENTS

 Safeguarding Policy
 Staff Code of Conduct Policy, Procedure and Documents
 Behaviour Principles Discipline Policy
 Disciplinary Policy, Procedures and Documents

## PROCEDURE

The following lays out the roles and procedures for e-safety of individuals and groups within High Street Primary School.

**Head Teacher**
The Head Teacher has overall responsibility for all matters relating to safety, including e-Safety. This responsibility includes ensuring that management is addressed through comprehensive policies and procedures that are effectively implemented and appropriately resourced within the overall financial position of the school.

**Senior Leadership Team**
Members of the Senior Leadership Team are responsible for ensuring that this policy is understood by all employees and fully implemented within their area(s) of responsibility.
They are responsible for ensuring that within their areas there are effective arrangements in place for the prompt reporting and management of any adverse incidents.

**IT Coordinator**
The leader of Information Technology is responsible for ensuring:
• That the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
• That the school meets the e-Safety technical requirements outlined in the Acceptable Usage Policy and any relevant guidance.
• That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed.
• The school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
• That the school keeps up-to-date with E-Safety technical information in order to effectively carry out its E-Safety role and to inform and update others as relevant.
• That any concerns raised over the use of the network/remote access/email will be investigated in accordance with the school policy.
• That monitoring software/systems are implemented and updated as agreed, in line with school policies.

**Employees**
Employees are responsible for ensuring that:
• They have an up to date awareness of e-Safety matters and of the current school E-Safety Policy and supporting documents.
• They report any suspected misuse or problem to the appropriate person, in line with the school policy.
• Digital communications with students via email should be on a professional level and only carried out using official school e-mail systems.
• E-Safety issues are embedded in all aspects of the curriculum and other school activities.
• They monitor ICT activity in lessons, extra-curricular and extended school activities.
• They are 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.
• In lessons where internet use is pre-planned learners are 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.

**Senior Designated Safeguarding Person**
The Senior Designated Safeguarding Person is the headteacher who has day-to-day responsibility for e-Safety, and is aware of the potential for serious safeguarding issues arising from:
• Sharing of personal data

• Access to illegal / inappropriate materials

• Inappropriate on-line contact with adults / strangers

• Potential or actual incidents of grooming

• Cyber-bullying


**Students**

• 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 and understand school expectations on the use of digital cameras and hand held devices. They should also know and understand the school rules on the taking / use of images and on cyber-bullying.