AIM high, GROW within and REACH beyond the stars

E-SAFETY POLICY
2024

Version	Date	Author	Changes

E-SAFETY POLICY

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, carers, visitors, external providers, work placements, students, contractors) who have access to and are users of school IT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head Teachers 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 cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

Roles and Responsibilities
The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Sub Committee receiving regular information about e-safety incidents and monitoring reports. E-Safety is within the Safeguarding Governor role. The Safeguarding Governor has regular meetings with SLT and school staff in charge of safeguarding protocols including E-Safety. The Safeguarding Governor reports back to the Governing Body.

Head Teacher and Senior Leadership Team

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Head Teacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Head teacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head Teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head Teacher and Senior Leadership Team work with an external Computer Support Team Officer designated to the school to ensure appropriate and rigorous software is in place to ensure safe IT practice in school.

E-Safety Team – IT Co-ordinator/HT/SBM/Schools ICT Service/Class Teachers:

- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place. To be reported to E-Safety Team.
- Ensures children are aware of E-Safety rules and safe practice
- Provides training and advice for staff.
- Liaises with the Local Authority/relevant body.
- Liaises with school technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments – all reportable items shared with the Schools ICT Service.
- Meets with the Computer Support Team Officer designated to the school to ensure appropriate and rigorous software is in place to ensure safe IT practice in school.
- Meets regularly to discuss current issues, review incident logs and filtering/change control logs and to enable reporting to Governors.

LinkIt Computer Support Team Officer:
The LinkIt Computer Support Team Officer are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements and any LA guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

- That they keep up to date with e-safety 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/internet/remote access/email is regularly monitored and new systems introduced in order that any misuse/ attempted misuse can be reported to the Senior Leadership Team and E-Safety Coordinator for investigation/action/sanction.

Teaching and Support Staff:

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 practices
- They have read, understood and signed the Staff Acceptable Use Policy.
- They report any suspected misuse or problem to the Senior Leadership Team or E-Safety Coordinator for investigation/action/ sanction.
- All digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum and other activities so that pupils understand and follow e-safety practices.
- E-Safety day takes place annually.
- E-Safety curriculum unit is delivered annually.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Staff monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- 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.
- Pupils know what to do if an inappropriate site appears.
- Staff know where to report site in order for protocols to be followed.

Child Protection/Safeguarding Designated Person

Should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding 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.
- Cyber-bullying.

E-Safety Networking

Hollyfast Primary School belongs to the Roots School Improvement Network Group and will:

- Work together to review the e-safety curricular provision – ensuring relevance, breadth and progression for each other's schools.
- Share good E-Safety practice, ideas and concepts.
- Work together as a staff group and with pupils to consider the impact of E-Safety and the advantages and disadvantages around internet use.

Pupils

Are responsible for using the school digital technology systems in accordance with the E-Safety rules: SMART:

  - S = Safe
  - M = Meeting
  - A = Accepting
  - R = Reliable
  - T = Tell

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Children having opportunity to work together from different schools to consider how to address issues such as cyber-bullying; sharing of personal data; inappropriate materials.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school as well as in school.
- Pupils are responsible for using IT systems in accordance with the Home School Agreement for IT use/ SMART protocol and signed.

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 including adhering to age related restrictions. The school will take every opportunity to

help parents understand these issues through parents' evenings, newsletters, letters, website and information about national and local e-safety campaigns and literature.
Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Their children's personal devices in the school.

Damage/loss

Parents/carers take full responsibility for the loan equipment issued to the pupil and are responsible for the equipment at all times whether on the school's property or not. If the equipment is damaged, lost or stolen, report to the school immediately on telephone 02476332521 and that parents/carers are responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, the police and the school must be informed immediately.

Use of 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, parents/ carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff only 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. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils 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 others without their permission
- 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.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Parents to complete an annual consent form for whether photographs of their children are allowed to be used for official events or publication including school website and school website or not to be used at all except on the schools secure pupil data system.
- Year six pupils are allowed to bring mobile phones to school but have to hand them into the school office at start of school and can collect at end of the school day.
- Surnames are not included in any publications.

General Data Protection Regulations

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR *(implemented May 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 school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA).
- Responsible persons are appointed to lead E-Safety Team.
- Risk assessments are carried out.
- It has clear and understood arrangements for the security, storage and transfer of personal data.
- Data subjects have rights of access and there are clear procedures for this to be obtained.
- There are clear and understood policies and routines for the deletion and disposal of data.
- There is a policy for reporting, logging, managing and recovering from information risk incidents.
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.
- There are clear policies about the use of cloud storage/cloud computing which ensure that such data storage, meets the requirements laid down by the Information Commissioner's Office as implemented by the LA IT Support Team.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must offer approved virus and malware checking software.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

Data held on portable devices must be transferred over to either the admin or curriculum server as soon as it is reasonably possible to do so. All data must then be deleted off the portable device.

Communication

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 should be aware that email communications are monitored.** Staff should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, texts or social media must not be used for these communications.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity:

The school has a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place. Protocols are clearly laid out in the School's Professional Code of Conduct distributed to all employees.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk.

School staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. Any concerns should be reported to the Designated Safeguard Lead/SLT immediately. Staff advised to follow Child Protection Policy procedures.

Illegal Incidents

- **If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, report immediately to the police and Designated Safeguard Lead.**

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant)
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
- other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed log should be retained by the group for evidence and reference.

Copies of the E-Safety Policy are available on the Health & Safety Notice Board with the master copy held by the SBM on behalf of the Head Teacher and Governing Body. This Policy was approved by the Head Teacher and the Chair of the Governing Body of Hollyfast Primary School July 2017. It will be reviewed during the 2020-2021 academic year.