**High Ercall Primary School**

******

***E-Safety Policy 2019***

|  |
| --- |
| **E-safety Policy- Document Status** |
|  |  | **Named****Responsibility** | Beatrice Cains (Safeguarding Governor) |
| **Date of review completion** |  | **Named****Responsibility** | Anna Edwards (ICT lead)K Matty (HLTA) |
| **Inception of new Policy**  | **October 2016** | **Named****Responsibility** | Sarah Roberts (Head) |
| **Date of Policy Adoption by Governing Body****Staff: PD Day – January 2017** | Full Governors: 6th December 2016  |

**Scope of the Policy**

6

This policy applies to all members of the High Ercall Primary Schoolcommunity (including staff, pupils, volunteers, parents / carers, visitors, community users) 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 Headteachers 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.

Keeping Children Safe in Education, statutory guidance for all schools, sets out a legal duty for Governing Bodies of all schools to ensure that there are appropriate filters and monitoring systems in place to safeguard all children.

At High Ercall Primary School, wewill deal with all incidents outlined within this policy and our anti-bullying policies. We will inform parents / carers of incidents of inappropriate E-safety behaviour that take place in and out of school.

**Roles and Responsibilities**

7

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 Governors receiving regular information about E-safety incidents and monitoring reports. A member of the Governing Body, Beatrice Cains, has taken on the role of E-safety Governor as part of their role as Safeguarding Governor. The role of the E-safety Governor will include:

• regular meetings with the Headteacher

• regular monitoring of E-safety incident logs

• regular monitoring of filtering

• reporting to the Governing Body through the Heads Report

**Headteacher:**

• The Headteacher has a duty of care for ensuring the safety (including E-safety) of members of the school community.

• The Headteacher and another member of the 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 Headteacher 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. Advice and external training to be sought as appropriate.

• The Headteacher 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 Senior Leadership Team will receive regular monitoring reports from the E-safety Co-ordinator.

**E-safety Coordinator:**

• leads the E-safety working group as required

• takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies and documents

• ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place

• provides training and advice for staff

• liaises with the Local Authority

• receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments

• meets regularly with E-safety Governor to discuss current issues, review incident logs and filtering

**Local Authority Technical staff:**

The Local Authority Technical Staff (Telford and Wrekin) 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 that may apply

• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

• 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 in order that any misuse / attempted misuse can be reported to the Headteacher / E-safety Coordinator for action

• that monitoring software / systems are implemented and updated

**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 Headteacher for action

• 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

• pupils understand and follow the E-safety and acceptable use policies

• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• in lessons where internet use is pre-planned pupils should be, where possible, 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

**Designated Safeguarding Lead:**

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

• sexting

Pupils:

**•** are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy

• 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 and understand the appropriate use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying

• should 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

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. The school will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, website and information about national / local E-safety campaigns and literature. Parents and carers will be expected 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

Community Users

Community Users who access school systems / website as part of the wider school provision will be expected to agree to and follow the Acceptable Use Policy which is explained upon receipt of any temporary passwords given.

11

Policy Statements

Education –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. Pupils need the help and support of the school to recognise and avoid E-safety risks and build their resilience.

E-safety is a focus in all areas of the curriculum and staff reinforce E-safety messages across the curriculum regularly. The E-safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided. Key principles are:

• A planned E-safety curriculum should be provided as part of PHSE and Computing lessons and should be regularly revisited

• Key E-safety messages should be reinforced as part of a planned programme of assemblies

• Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line 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

• Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school

• Staff should act as good role models in their use of digital technologies the internet and mobile devices

• In lessons where internet use is pre-planned, it is best practice 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

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

• It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) 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.

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 monitoring and 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:

• Letters, newsletters, twitter and web site

• Parents / Carers workshops

• High profile events and campaigns eg Safer Internet Day

Education & Training – Staff / Volunteers

It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal E-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-safety training needs of all staff will be carried out regularly.

• All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Agreements

• The E-safety Coordinator will receive regular updates through attendance at external training events

• This E-safety policy and its updates will be presented to and discussed by staff in staff meetings and PD days

• The E-safety Coordinator will provide guidance and training to individuals as required.

Training – Governors

Governors should take part in E-safety training and awareness sessions. This may be offered in a number of ways:

• Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation

• Participation in school training

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities:

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

• There will be regular reviews and audits of the safety and security of school technical systems

• Servers, wireless systems and cabling must be securely located and physical access restricted

• All users will have clearly defined access rights to school technical systems and devices

• All users in KS2 will be provided with a username and secure password. Users are responsible for the security of their username and password

• The administrator passwords for the school ICT system, used by the Network Manager must also be available to the Headteacher and kept in a secure place

• The Headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

* Internet access is filtered for all users.

• The school has provided differentiated user-level filtering

• E-safety Coordinator regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement

• An appropriate system is in place for users to report any actual / potential technical incident / security breach

• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software (provided by Local Authority Technical Team)

• An agreed policy (see Visitors in Schools Policy) is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems

• An agreed policy is in place regarding the extent of personal use that staff users and their family members are allowed on school devices that may be used out of school (see Staff Handbook)

• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

**Bring Your Own Device (BYOD)**

We do not permit any use of personal devices for pupils during school hours. Any devices that are brought to school for use out of school hours should be handed in to a member of staff to be stored securely in the school office.

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, 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 students / pupils in the digital / video images.

• Staff and volunteers 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 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.

• Written permission from parents or carers is obtained for photographs of pupils to be published on the school website or on the internet on sites such as twitter.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulations 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 ensures 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.
* All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
* It has a Data Protection Policy
* It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

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 should be encrypted and password protected, or kept secure

**•** the device should be password protected

**•** the device must offer approved virus and malware checking software

16

**•** the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. 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

• Users must immediately report, to the nominated person, 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 etc) must be professional in tone and content

Social Media

The school has adopted the Telford and Wrekin Council Social Media Policy.

**Reporting Incidents**

Reporting of incidents will follow the school’s Safeguarding Procedures. Where digital content is involved, these additional steps will be taken.

* 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 abuse – see below)
* 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.

**Schedule for Development / Monitoring / Review**

5

|  |  |
| --- | --- |
| The implementation of this E-safety policy will be monitored by the: | *Headteacher Mrs S Robert**E-safety Officer Mrs S Roberts* *IT Subject Leader Mrs A Edwards,* *HLTA Mrs K Matty* |
| Monitoring will take place at regular intervals: | *Annually**Within Governor termly monitoring through the Termly Development plan* |
| The *Governing Body* will receive a report on the implementation of the E-safety policy generated by the monitoring group (which will include anonymous details of E-safety incidents) at regular intervals: | *Head’s Report each term* |
| The E-safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-safety or incidents that have taken place. The next anticipated review date: | *Autumn 2020* |
| Should serious E-safety incidents take place, the following external persons / agencies should be informed: | *Police, Family Connect*  |

**The school will monitor the impact of the policy using:**

• Logs of reported incidents (Concern/Incident Form)

• Monitoring logs of internet activity (including sites visited) through Sensio

• Surveys / questionnaires of

• pupils

• parents / carers

22