**Eastfield Online Safety Policy**

At Eastfield Primary School we believe that all children and adults in our school and community are important. We aim to provide an environment where everyone feels valued, happy and secure. We are committed to enabling all of our pupils to access their education successfully by regulating the conduct of all pupils.

**Review of this Policy**

4

This Online Safety policy has been developed by the computing lead and senior leadership team of Eastfield made up of:

* Headteacher
* Senior Leaders
* Computing leadership

|  |  |
| --- | --- |
| The implementation of this Online Safety policy will be monitored by the: | Ashley Girt – Computing lead Ruth Ellis - Headteacher |
| Monitoring will take place at regular intervals: | Once a year |
| Local Advisory Board will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals: | Once a year |
| The Online 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 online safety or incidents that have taken place. The next anticipated review date will be: | 1st September 2021 |
| Should serious online safety incidents take place, the following external persons / agencies should be informed: | Bradgate Educational Partnership, LA Safeguarding Officer, LADO, Police |

**Aims**

Our school aims to:

* Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
* Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
* Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**Scope**

This policy is based on the Department for Education’s statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on [preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation). It also refers to the Department’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the [National Curriculum computing programmes of study](https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study).

This policy complies with our funding agreement and articles of association.

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / school digital technology 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 behavior of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behavior. This is pertinent to incidents of online-bullying or other Online 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 (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behavior Policy.

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

**Roles and responsibilities**

The Headteacher

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing lead .

The Headteacher and (at least) another member 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.

The Headteacher and Senior Leaders are responsible for ensuring that the Computing Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles. The BEP will be informed of any data breaches and online safety issues to ensure the correct procedures are carried out.

The Senior Leadership Team will receive regular monitoring reports from the Computing lead.

The Designated Safeguarding Lead

Details of the school’s designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSLs takes lead responsibility for online safety in school, in particular:

Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

Network Manager and Technical staff

The Network Manager, Technical Staff and Computing lead is 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 online safety technical requirements and any Local Authority, and BEP guidance 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 (if it has one), 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 online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
* That the use of the network, internet, Learning Platform, remote access and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher and Senior Leadership team for investigation.
* That monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

* They have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices
* They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
* They report any suspected misuse or problem to the Headteacher Senior Leadership team and DSL) for investigation.
* All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
* Online safety issues are embedded in all aspects of the curriculum and other activities. All teachers to teach yearly units on online safety.
* Students / pupils understand and follow the Online Safety Policy and acceptable use policies
* Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
* They 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

Students / Pupils:

* Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement.
* 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online bullying.
* Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the schools Online 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 and local online safety campaigns and literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

* Digital and video images taken at school events
* Access to parents’ sections of the website and on-line student / pupil records
* Their children’s personal devices in the school.

Many parents and carers have only 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 the children’s online behaviors. 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 raise parents’ awareness of internet safety in letters or other communications home, and in information via our website or twitter feed .This policy will also be shared with parents.
* Online safety will also be covered during parents’ evenings and information evenings regarding online safety.
* If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or a member of the Senior Leadership Team.
* Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

**Educating pupils about online safety**

Pupils will be taught about online safety as part of the curriculum.

In Key Stage 1, pupils will be taught to:

* Use technology safely and respectfully, keeping personal information private
* Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

* Use technology safely, respectfully and responsibly
* Recognise acceptable and unacceptable behaviour
* Identify a range of ways to report concerns about content and contact
* Educating parents about online safety

**Cyber-bullying**

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behavior policy and social media policy)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behavior policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavors to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

**Technical – infrastructure / equipment, filtering and monitoring**

The school will be responsible for ensuring that the school network 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 online 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.
* The network manager who will keep an up to date record of users and their usernames will provide all users (at KS2 and above) with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password every term.
* The administrator passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (school safe)
* The network manager 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. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
* There is a clear process in place to deal with requests for filtering changes.

Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. Educating young people about the risks of extremism, particularly in a digital age, has long been a priority for many schools. The Counter Terrorism & Security (CTS) Act 2015 has now made placed a [statutory duty](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/417943/Prevent_Duty_Guidance_England_Wales.pdf) for schools to show “due regard to the need to prevent people from being drawn into terrorism”.

* The school has provided enhanced user-level filtering
* School technical staff 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 (CPOMS) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
* 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.
* An agreed policy is in place (The acceptable use policy) for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.
* An agreed policy is in place (The acceptable use policy) that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
* An agreed policy is in place (The acceptable use policy) 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.

**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 at the beginning of every year.

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 e.g. on social networking sites.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press this is agreed with the parents at the beginning of the child’s education at Eastfield. If parents wish to amend this then they may do so by letting the school know via schools office or email.

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 in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be 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 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 / school equipment, the personal equipment of staff should not be used for such purposes.
* Care should be taken when taking digital / video images that students / 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.
* Pupil’s work can only be published with the permission of the student / pupil and parents or carers.

**Acceptable use of the internet in school**

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet. Visitors will be expected to read and agree to the school’s terms on acceptable use if relevant.

Use of the school’s internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual’s role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements at the end of this document.

* Pupils using mobile devices in school
* Pupils may bring mobile devices into school, but are not permitted to use them during school hours
* Any use of mobile devices in school by pupils must be in line with the Mobile Phone Policy (2018) found at the end of this document.
* Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

**Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school’s terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the computing lead or network manager.

Work devices must be used solely for work activities.

**Data protection**

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) [announced in 2016](http://ec.europa.eu/justice/data-protection/). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data

In order to operate efficiently Eastfield Primary School has to collect and use information about people with whom it works and the pupils it provides an education to. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

The School is committed to ensuring personal data is properly managed and that it ensures compliance with current data protection legislation. The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so. Further information on this can be found in the schools data protection policy (2018)

**Social Media**

Eastfield have 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. Pupils and Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the s/ school or local authority / BEP liable to the injured party. Reasonable steps to prevent predictable harm are in place.

Eastfield provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

* Ensuring that personal information is not published
* Training is provided including: 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 students / pupils, parents / carers or school / 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 / BEP
* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
* When official school social media accounts are established there should be:
* A process for approval by senior leaders. See the schools Twitter Policy (2018)
* Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
* A code of behaviour for users of the accounts, including
* Systems for reporting and dealing with abuse and misuse
* Understanding of how incidents may be dealt with under school / school disciplinary procedures
* Personal Use:
* Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or affects the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
* Personal communications which do not refer to or impact upon the school are outside the scope of this policy
* Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken See disciplinary procedures
* Monitoring of Public Social Media
* As part of our active social media engagement we pro-actively monitor the Internet for public postings about the school
* The school effectively respond to social media comments made by others according to a defined policy or process

**E-mail**

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

The school gives all staff & governors their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Links with other policies:

This online safety policy is linked to our:

* Child protection and safeguarding policy
* Behavior policy
* Staff disciplinary procedures
* Data protection policy and privacy notices
* Complaints procedure
* Twitter Policy
* Mobile phone policy
* Acceptable use policy

Acceptable Use Policy

The school has the responsibility of providing you with safe, reliable and useful ICT resources (network, Internet Access, Learning Platform etc) that will help you make the most of opportunities for administration, teaching and learning. You have a right to these resources. With this right however, come the following responsibilities. I understand that the School may check my computer files, may monitor the Internet sites that I visit and my emails. If I do not follow these guidelines the AUP will be enforced.

I will read and follow the guidelines in this AUP. I will take responsibility for my own use of all ICT making sure that I use technology safely, responsibly and legally. This means:

* I will take personal responsibility for my awareness of the opportunities and risks posed by new technologies. I will make pupils in my care aware of e-safety measures.
* I acknowledge that my ICT equipment usage is monitored and recorded for the protection of myself and others I work with.
* I will use always use my school email for professional purposes. I will only use email systems, chat rooms and other messaging methods that are approved by the school. I will never use ICT for bullying or harassing others or in a way that will bring the school into disrepute.
* I will only download or install any software or files on school’s ICT equipment as agreed with the school’s technical/ICT staff. I will be careful opening e-mails and attachments from unknown people.
* If I have to use a flash drive (USB memory stick) in school I will a run an anti-virus check on it every time.
* I will not intentionally gain access to unsuitable or illegal sites eg pornography, child abuse, racism, incitement to violence. I will report as soon as possible accidental access to such sites. I understand that my report will be confidential and would protect other members of the school community.
* I will only access computer systems using my own login and password, which I will keep secret. I realize that if I access files that are not my own without permission (hacking) I will be breaking the Computer Misuse Act 1990.
* I will ensure that my work does not break The Copyright, Design and Patents law. I will always acknowledge the source of information (words, images etc) I use. I will not copy other people’s work and pass it off as my own (plagiarism).
* I will use school ICT equipment with care and report any damage which occurs as soon as possible.
* I will use network resources responsibly e.g.
* I will only print when necessary
* I will regularly review my files and delete them when no longer needed
* I will only store school-related files and images on the school network
* I will only use the ICT equipment for school related work

Signed: Date: