Warren Farm Primary School

E-Safety Policy 2022

Date of Last review	14/09/2022
Date agreed by governors	10/11/2022
Date of next review	10/11/2023

Warren Farm Primary School eSafety Policy

Our Vision

Warren Farm Primary School embraces the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. We are also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, Warren Farm School aims to provide a safe and secure environment which not only protects all people on the premises but also educates them on how to stay safe in the wider world.

Scope

This policy and related documents apply at all times to fixed and mobile technologies owned and supplied by the School and to personal devices owned by adults and young people while on the school premises.

Related Documents:

Acceptable Internet Use Policy

Data Protection Policy
Freedom of Information Policy
Behaviour Policy
Special Needs Policy
Anti-Bullying Policy
Birmingham City Council Internet Use Policy, Internet Use Code of Practice and Email Use Policy (linked from www.bgfl.org/esafety)

Publicising e-SafetyEffective communication across the School community is paramount to achieving the School vision for safe and responsible citizens. To achieve this we will: Make this policy, and related documents, available on the School website Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated or reviewed.

Roles and Responsibilities

In this document, the term staff refers to all employees of the School, adults that work with the school, such as, Adults in training (teachers, support staff), visitors and supply staff using new technologies on site.

The Head and Governors have ultimate responsibility for establishing safe practice and managing e-Safety issues at our School. The role of DSP has been allocated to Mrs Gillian Barr

(Head Teacher), Mrs Catherine Osborne (Deputy Head) and Mrs Kathryn Taroni (Assistant Head). They are the central points of contact for all e-Safety issues and will be responsible for day to day management.

All members of the School community have certain core responsibilities within and outside the School environment. They should:

- Use technology responsibly
- Accept responsibility for their use of technology
- Model best practice when using technology
- Report any incidents to the e-Safety coordinator using the school procedures
- Understand that network activity and online communications are monitored, including any personal and private communications made via the School network.

Be aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action

Additional roles and responsibilities are discussed in the Becta document – AUP's in context: Establishing safe and responsible behaviours, also available at http://www.bgfl.org/esafety. These will be communicated to the relevant groups at appropriate times.

Physical Environment / Security

The School endeavours to provide a safe environment for the whole community and we review both physical and network security regularly and monitor who has access to the system consulting with the LA (Local Authority), where appropriate.

- Anti-virus software is installed on all computers and updated regularly
- Central filtering is provided and managed locally. We use the Smoothwall filtering system. All staff and students understand that if an inappropriate site is discovered it must be reported to the e-Safety Co-Ordinator/DSP, who will report it to the SBM / IT Technician to be blocked. All incidents will be recorded via Smotthwall for audit purposes.
- Requests for changes to the filtering will be directed to the e-Safety Co-ordinator in the first instance who will forward these on to the IT Technician or SBM or liaise with the Head as appropriate.
- Pupils' use is monitored by staff within that lesson and Smoothwall.
- Central Staff use is monitored by Smoothwall
- All staff are issued with their own username and password for network access. Visitors/Supply/Contracted staff are issued with temporary ID's and the details recorded in the school office
- All pupils have their own username and password and understand that this must not be shared

Mobile / Emerging Technologies

- Staff at the School are provided with a laptop for educational use and their own professional development. All staff understand that the Acceptable Use Policies apply to this equipment at all times.
- To ensure the security of the School systems, personal equipment is currently not permitted to be connected to the school network.
- Staff understand that they should use their own mobile phones sensibly and in line with School policy and not to contact parents or pupils using their personal phone, the School phone should be used.
- The Educations and Inspections Act 2006 grants the Head the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head will exercise this right at their discretion.
- Pictures/video's of staff and pupils should not be taken on personal devices.
- New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the School community

E-mail

The School e-mail system is governed by the school E-mail Policy:

- All staff are given a School e-mail address and understand that this must be used for all professional communication.
- Everyone in the School community understands that the e-mail system is monitored and should not be considered private communication.
- Guidance is given to the School community around how e-mail should be structured when using school e-mail addresses.
- Staff are allowed to access personal e-mail accounts on the school system outside directed time and understand that any messages sent using the School equipment should be in line with the e-mail policy. In addition, they also understand that these messages will be scanned by the monitoring software.
- Everyone in the School community understands that any inappropriate e-mails must be reported to the class teacher / e-Safety Co-Ordinator as soon as possible.

The Head takes responsibility for content published to the school web site but delegates general editorial responsibility to e-Safety Co-Ordinator/DSP. Class teachers are responsible for the editorial control of work published by their students.

- The School will hold the copyright for any material published on the School web site or will obtain permission from the copyright holder prior to publishing with appropriate attribution.
- The School encourages the use of e-mail to contact the school via the school office / generic e-mail address.

- The School does not publish any contact details for the pupils.
- The School encourages appropriate, educational use of other technologies and where possible embeds these in the School web site or creates a School account on the site.

Digital Media

We respect the privacy of the School community and will obtain written permission from staff; parents, carers or pupils before any images or video are published or distributed outside the School. Instructions from Parents/Carers regarding this is stored at the School Office.

- Photographs will be published in line with Becta guidance and not identify any individual pupil.
- Students' full names will not be published outside the School environment.
- Written permission will be obtained from parents or carers prior to pupils taking part in external video conferencing.
- Staff must never use mobile telephones in school when children are present.

Social Networking and Online Communication

The School is reviewing the use of social networking sites and online communication and currently does not allow access to any inappropriate sites.

Unmonitored or not moderated chat sites present an unacceptable level of risk and are blocked in School. Pupils are given age appropriate advice and guidance around the use of such sites as necessary.

Educational Use

School staff model appropriate use of School resources including the internet.

- All activities using the internet, including homework and independent research topics, will be tested first to minimise the risk of exposure to inappropriate material. Staff should not search for sites not previously researched in front of pupils.
- Where appropriate, links to specific web sites will be provided instead of open searching for information.
- Students will be taught how to conduct safe searches of the internet and this information will be made available to parents and carers.
- Teachers will be responsible for their own classroom management when using ICT equipment and will remind pupils of the Acceptable Use Polices before any activity.
- Staff will be expected to reference all third party resources that are used.

E-safety training

The School offers continuing professional development that includes whole School inset.

- There is an induction process and mentor scheme available for new members of staff.
- Educational resources are reviewed by Heads of Department and disseminated through curriculum meetings, staff meetings and training sessions.
- E-Safety is embedded throughout the school curriculum and visited by each year.
- Pupils are taught how to validate the accuracy of information found on the internet.
- Parents are offered e-Safety advice and guidance.

Data Security / Data Protection

Personal data will be recorded, processed, transferred and made available in accordance with the Data Protection Act 1998. We will also comply with the requirements of the GDPR from May 2018.

Equal Opportunities/Inclusion

All pupils matter and are given every opportunity to achieve their best. We achieve this by planning appropriately to meet the needs of all of our pupils including those with Special Educational Needs, those who are Gifted and Talented and all pupils from all social, cultural and ethnic backgrounds.

We meet the needs of all pupils through:

- Providing resources that reflect diversity and are free from discrimination and stereotyping.
- Using a range of teaching and learning strategies based upon the pupils individual needs.
- Ensuring access to every activity where it is safe and legal to do so.

Responding to Incidents

Inappropriate use of the School resources will be dealt with in line with other School policies e.g. Behaviour, Anti-Bullying and Child Protection Policy.

- Serious breaches of this policy by students will be treated as any other serious breach of conduct in accordance with School Behaviour Policy. Referrals to the Heads of Department/Heads of Year may be appropriate at this level. For all serious breaches, the incident will be fully investigated, and appropriate records made on personal files with the ultimate sanction of exclusion reserved for the most serious of cases.
- Minor student offences, such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the School Behaviour Policy.
- The Educations and Inspections Act 2006 grants the Head the legal power to take action against incidents affecting the School that occur outside the normal School day and this right will be exercised where it is considered appropriate.
- Any suspected illegal activity will be reported directly to the Police and/or CEOP.

Whatever happens, the following points are very important to remember:

- It is not appropriate to rely on computer settings and filtering.
- In the UK, if you come across illegal (or suspected illegal) websites or content these should be reported to the Internet Watch Foundation www.iwf.org.uk
- Reports about suspicious behaviour towards children and young people in an online environment should be made to the Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk. Law enforcement agencies and the service providers may need to take urgent steps to locate the child and/or remove the content.
- The most important safeguarding measure is the education in the safe use of technology. Not only educating the child, but also educating the adult. Children should be empowered from a young age to understand the risks and issues.
- If you or a pupil come across a website which you think may have illegal content, NEVER investigate.
- NEVER forward content (email, photo, website address etc.) to someone else containing inappropriate content.
- NEVER forward content (email, photo, website address etc.) to someone else containing illegal content; this is an offence.

Some Things You Should Know – Committing an Illegal Act

- Receiving unsolicited emails containing illegal content is not an offence (on the part of the receiver).
- Do not open the content or investigate yourself, this is an offence (possession). Showing somebody else the illegal material is an offence (distribution).
- Printing a copy of the material is an offence (producing).

If you are suspicious or just not sure, don't take the risk. Report it immediately to the Head Teacher to make a decision as to whether to involve the Police. The Head Teacher should NOT look at it but should act on your explanation and judgment.

Always remember the 4 most important points:

Find it

Report it

Action it

Log it