FAIRFIELD COMMUNITY PRIMARY SCHOOL

Aiming for Happiness and High Standards

Online Safety Policy

Mission Statement

At Fairfield Community Primary School, we aim to provide a safe, secure environment which will promote ***Happiness and High standards****.*

We aim to meet the needs and celebrate the achievements of all pupils, who, through high expectations and high standards of teaching will reach their own potential regardless of ability.

We offer equal opportunities to all in the belief that Fairfield children will take their places as productive, valued and tolerant members of society.

Introduction

The internet holds a wealth of up-to-date information. There are many ways to improve communication including email, blogging and social media. Within school the internet is used in many ways through the use of a range of hardware and software. However, through the use of the internet, all users (including Senior Leadership Team (SLT), board of governors, all staff, visitors and pupils) need to be aware of the risks in using it or other technologies. This policy recognises the risks of using the internet with other software and hardware and our commitment to avoiding these risks. We want to make sure that children are prepared for using technology as an integral part of life in the future. Both this policy and the Acceptable Use policy (for all staff and children) outline use of the internet, software (programs and applications used within school) and hardware (e.g. laptops, tablets (iPads), cameras and TVs).

The school will reserve the right to become involved in any incidents outside of school times if it impinges on life within school even if the use of the medium concerned does not breach legal boundaries.

Aims

- To keep children safe from vulnerability that the internet can create.
- To advise children against the inappropriate use of websites.
- To prevent children being in contact with any unsuitable party.
- For children to calculate risk effectively.
- To prevent bullying, grooming, radicalisation, terrorism, exploitation and extremism.
- To ensure children and staff are kept safe and confident about using technology.
- To use SMART (safe, meet, accept, reliable and tell) targets to keep safe online

Roles and Responsibilities

This policy was completed in:
The policy was completed by:
The policy was completed in association with:
The online safety lead is:
The policy was approved by the governing body in:

Guidance acknowledged and included within our online safety policy:

http://greatermanchesterscb.proceduresonline.com/chapters/p_sg_ch_yp_online.html

http://www.safeguardingburychildren.org/index.aspx?articleid=8916

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/457037/Inspecting_safeguarding_in_early_years_education_and_skills_settings.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/447595/KCSIE_July_2015.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/439598/prevent-duty-departmental-advice-v6.pdf

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458866/School_inspection_handbook_section_5_from_September_2015.pdf

Using the school network and equipment

- The school network is monitored securely by Bury Council filters and backed up securely (maintained by PCEductech).
- Users must access the school network using their own logins provided per staff member, or class for children. Visitors (e.g. supply teachers) also have a temporary log on. Staff are advised on using secure passwords. Passwords to these are not to be shared.
- Users should not attempt to log on or access other user's information without permission.
- Software or programs should not be installed or downloaded without prior permission from Computing lead.
- Any hardware brought into school needs to be scanned before use with a school based machine.
- Machines should not be left logged in and unattended. Hardware needs to be logged out when leaving the machine for a period of time.
- All hardware needs to be logged out, shut down and locked away at the end of each working day.
- The wireless network needs to be encrypted to prevent outside use.

- Administration rights for the network are strictly for the Computing lead and technician maintaining the network (PCEdutech). Any changes needs to be reported using request for technical support in school office.
- Staff are allowed to take equipment of school premises. Permission needs to be granted and equipment logged out in school office. Equipment needs to be stored securely when not in school.
- Remote access (offsite) is only granted to users when permission is given by the head teacher. Access to the school network from non-school based users is unauthorized.
- When a staff member leaves, their account is deleted.
- If equipment needs to be destroyed, it is to be reported to the technician through the school office.
- A full school inventory of all equipment is logged and annually checked.

Using the internet

The benefits to using the internet educationally outweigh the risks. The internet can be used for supporting teaching of the curriculum, using systems to support the running of the school and electronic communication across staff members with other agencies or the LA.

- Web filtering of the internet is provided by Bury Local Authority. This means that all content is filtered to prevent illegal content as best possible.
- Through our Acceptable Use policy for children, children are made aware of the risks and their responsibility when using the internet within school. Staff are made aware of their responsibility when using the internet through the Staff Acceptable Use policy. Staff members are supplied with their own, or access to a, laptop where activity can be monitored and checked.
- All staff members are provided with a school based email (example@buryla.org). This is to be used for professional and school related matters only. Emails should be professional and the good impression of the school maintained. Staff are not permitted to use personal emails for conducting school business or sending school related information.
- When using email, it is the responsibility of the account holder to attach a disclaimer stating 'the views expressed are not necessarily those of the school or Local Authority'.
- It is the responsibility of the staff member to make sure their password is secure and not shared with anyone.
- Children are taught about emailing safely and appropriately as part of the curriculum.
- Staff and pupils are not permitted to communicate via electronic communication (e.g. email, social media etc.) unless part of a teaching lesson use child appropriate software.

- Accidental access (by staff or children) to inappropriate content (e.g. racist, sexual or abusive material) on the internet is to be reported so that it can be blocked via Bury LA.
- If users (either adult or child) receive offensive emails (including bullying), they are to be reported to the headteacher immediately and investigated.
- Anti-virus software is on all machines. No downloads are allowed without permission.
- The use of social media, chatrooms, online gambling sites are not permitted.
- Children are taught the risks of being online. This includes: not using sites without permission, not putting personal information or images online, understanding privacy rules on any profiles, being cautious of information on the internet and its validity or truth.

Use of mobile devices

- Staff are allowed to bring in personal mobile phones but these are not permitted to be used for school business. Staff are not permitted to contact parents or children using personal devices. Personal devices are to be switched off or on silent during the day. Staff are permitted to use personal devices during breaks or before or after the school day. No personal devices are to be left where children can access them.
- Children are allowed to bring in personal phones with permission but these are to be collected by the teacher at the beginning of the day and returned at the end of the day.
- Prior permission from the headteacher must be given for staff to use their personal devices within school for teaching purposes or off site, for example trips. However, in this case images must be transferred immediately onto the school network and deleted from any personal device.
- Written consent from all parents/carers of pupils must be gained annually before photographing any child as found on contact forms in the blue files in the office.
- When taking photographs, they must be stored on the school network (Media Drive) and deleted of mobile devices as soon as possible. It is not permitted for any school photographs, videos or sensitive information to be stored on personal mobile devices or taken home.
- Children may use a personal disposable camera when on trips but are reminded this is for personal use only.
- Parents may use personal devices for photographing (e.g. in assembly) but are reminded this is for personal use only.
- Webcams or video calling may be used within school but must be used with an adult present. Children and adults are reminded of the professional conduct that must be upheld when representing the school to other schools or professionals.

Website

- The school website must be checked regularly to make sure no information or images have been uploaded inadvertently that put staff or children at risk.
- Before uploading anything onto the website, it must be checked by one of the Senior Leadership Team.
- All staff need to be aware of children who are not permitted to be photographed. If unsure please check with EW or contact forms found in blue files in the office.
- Copyright and Data Protection must be respected.
- Sensitive or personal information relating to staff or children is not to be uploaded onto the website.
- Photos of children must not be posted alongside names of children.

Reporting Incidents for both staff and pupils

- All online safety incidents (e.g. cyberbullying, extremism, grooming etc.) are reported to the headteacher to be reviewed or investigated following safeguarding procedures.
- Any incidents where staff or pupils do not follow the Acceptable Use Policy will be reported to the headteacher and dealt with following school policy for behaviour or if necessary disciplinary.
- Incidents where there is a risk to the school safety (e.g. data) will be reported to the headteacher and technical advice will be sought if necessary.
- School equipment, software, network usage and internet usage will be monitored.

Appendices

- Acceptable Use policy staff
- Acceptable Use policy children
- Safeguarding policy
- British Values policy