Dimple Well Infant School

E-Safety Policy

2020

E-Safety Policy

E-Safety is all about how to stay safe online. It is taught as part of the Computing curriculum and is taught all year long. Wherever possible the school will try to take part in national campaigns such as Safer Internet Day. The policy and its implementation will be reviewed annually. The policy runs alongside other school policies including those for Computing, Social Media, Anti-Bullying, Health and Safety and Child Protection.

Staff

- All staff will be given a copy of the E-Safety Policy and its importance explained.
- All staff must sign to confirm they have read the school's Acceptable Use Agreement and policies.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All laptops and portable devices issued to a member of staff remain the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to internet access, data protection and use of software.
- Staff will use a child friendly safe search engine when accessing the web with pupils e.g. Google Safe Search.
- 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 Policies.
- E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Computing Subject Leader and Headteacher will provide advice / guidance / training as required to individuals as required

Parents

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, the school website and on the parent hub.
- The school will provide E-Safety links and advice for parents/carers on the school website.
- An E-Safety newsletter will be sent to parents termly, keeping them up to date with any developments.
- School will seek parental permission annually from parents, via a 'Pupil Information sheet, before children are allowed to use the internet. They will also

be asked for permission to use photographs of their children on the school website and social media channels.

System security

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- School ICT systems security will be reviewed regularly.
- Virus protection is installed on all appropriate hardware and will be kept active and updated.
- Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems.
- A secure and robust username and password convention exists for all system access (email, network and home access)
- All staff have a responsibility for the security of their usernames and passwords for systems and applications. Users must not allow others to access systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Anyone inadvertently accessing inappropriate material should immediately inform the Computing Subject Leader and Headteacher or designated person in school and ensure that the incident is recorded.

Managing filtering

- The school uses a filtered internet service provided by RM Education which includes age appropriate filtering. The school will continue to work with Wakefield LA and other bodies to ensure systems to protect pupils are reviewed and improved and report any issues.
- If pupils or staff discover any unsuitable site, it must be reported to the Computing Subject Leader and Headteacher and be logged.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Protecting personal data

- Dimple Well will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 2018 (DPA 2018), and the General Data Protection Regulation (GDPR) commitments.

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 as outlined in the Data Protection policy.
- Staff must not keep confidential information on removable devices such as USB devices unless suitably security protected through encryption.
- All computers have an automatic lock set up, which requires the password to be re-administered if not used for 15 minutes; computers that are used to access sensitive information should also be locked (Ctrl-Atl-Del) when unattended.
- Staff will not leave personal and sensitive printed documents on printers within public areas of the school.
- Portable devices issued to staff such as iPads and the school mobile phone must be secured by PIN.

Handling E-Safety complaints

- Complaints of internet misuse by children will be dealt with by the Computing Subject Leader in conjunction with the Headteacher and deputy headteacher. Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- All incidents must be logged on the orange E-Safety slip (can be found on the safeguarding display)

Community use of the Internet

- External organisations using the school's ICT facilities must be made aware of and adhere to the E-Safety Policy .
- Visitors and supply teachers should be provided with a supply login once they have signed an acceptable use policy. Staff must not log visitors into their own accounts.

Technical staff

- The technical staff is responsible for ensuring:
- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's networks through a properly enforced password protection policy,
- that they keep up to date with e-safety technical information in order to effectively carry out their role and to inform and update others as relevant
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher

- 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 E-Safety matters and of the current school E-Safety policy and practices
- they have read, understood and signed the Acceptable Use Policy
- they report any suspected misuse or problem to the Head teacher or Computing Subject Leader
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school E-Safety and Acceptable Use Policy
- they monitor computing activity in lessons