The Orchards

E-Safety Policy

Policy Version			
Date	**Document Version**	**Document Revision History**	**Document Author/Reviser**
18/06/2019	1		HOB

This policy will be reviewed every 12 months or in light of a change to local and Government legislation.

The Dunham Trust's Vision, Aims and Ethos

Together we will
Challenge the ordinary
Promote individuality
Be advocates for change

Across our schools we encourage cross-collaboration and the sharing of best practice. We believe that we are able to help our schools and their young people to aspire to, and achieve, success. We are committed to ensuring that every child and young person has a pathway to succeed and that:

- gives the best possible start in life
- equips them with creativity, spirit and confidence
- enables individuals to appreciate life and equip for further learning
- supports the child in becoming a responsible citizen and contribute to the local community
- celebrates the individual

The Dunham Trust aims to contribute positively to the self-improving school-led system in education across this locality. We believe in true collaboration; working in partnership, investing in people and building capacity for long term, sustainable success. There is both the expectation and opportunity for collaboration across individual Trust schools.

The five schools in The Dunham Trust are:

Acre Hall Primary School
Barton Clough Primary School
Elmridge Primary School
The Orchards Special School
Lime Tree Primary Academy

The Dunham Trust is a growing Trust with very clear educational aims and expectations. One of The Trust's primary aims is to transform the schools within The Trust into sustainable learning communities. We want to create a community of good and outstanding schools with the highest aspirations. The skills and expertise that exist within The Trust will ensure that our academies and young people aspire to, and achieve, success. We achieve this through a well-structured School Improvement Programme which is supported by The Trust's two Teaching Schools.

Introduction

E-Safety encompasses internet technologies and electronic communications such as laptops, tablets, mobile telephones and wireless technology. Use of the Trust's ICT equipment by any members of the community must be in accordance with this policy. Any use which infringes this policy will be treated very seriously by the Trust Board and Local Governing Body. This E-safety policy will operate in conjunction with other policies including those for Positive Response, Anti-Bullying, Teaching and Learning, Data Protection and Security.

Teaching and Learning - The Importance of Internet use in Education

The internet is an essential element in 21st life for education, business and social interaction. The Trust has a duty to provide children with quality Internet access as part of their learning experience.

Safeguarding children against any inappropriate material is a priority across school. All staff are aware of and have received updated Prevent training which deals with the issue of potential radicalisation and how to identify any possible signs of this.

Internet use is part of the statutory curriculum and a necessary tool for staff and children. The purpose of Internet use in school is to raise educational standards, to promote children's achievement, to support the professional work of staff and to enhance the school's management information systems.

Using the Internet to Enhance Learning

Internet access in school will be designed expressly for children use and will include filtering arrangements appropriate to the age and needs of the children.
The Orchard's Specialist School manages its own internet and content filtering provision. The school's internet service provider is esi – tech and the school's content filtering and firewalls are provided by Sophos.

The school's email system is purchased through Trafford Council's LA ICT Team.

The school's networks that can connect to the internet are:
1. A wired Local Area Network (LAN). This is a secure network where the school's servers, data, management information systems and active directory sits. Access to this network is only for school provided equipment – classroom computers, office computers and staff laptops
2. A secure staff wireless network – Staff Only Devices – this is restricted to school owned staff laptops and tablets. Internet usage is strictly filtered, with the same group policy as the LAN, and is password controlled. Individual activity is recorded by Sophos and can be monitored

Children will be taught in their lessons what Internet use is acceptable and what is not and given clear objectives for Internet use, where appropriate. Where not appropriate, adults will ensure that use of the internet is monitored.

Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the learning needs of the children.

E-Mail

The school's e-mail system is for staff use only. New e-mail accounts can only be set up with the authorisation of the Head of School. The list of open e-mail accounts is reviewed on a termly basis by the Personnel and HR manager to ensure that they are still valid for staff working at the school.

No personal details of any child/staff member, such as address or telephone number, should be revealed, without specific permission and no one should arrange to meet anyone in any e-mail communication.

Esi-tech have confirmed that their systems are GDPR compliant.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

E-mails sent to an external organisation should be written carefully and authorised before sending in the same way as a letter written on school headed notepaper.

Children and staff should use the school email system for work and educational purposes and NOT for personal chat or for social networking.

Staff should only use their school email when communicating with parents and families.

The forwarding of chain letters is not permitted.

Managing Filtering

The school will work in partnership with its Internet Service Provider to ensure systems to protect children and staff are reviewed and improved.
If staff or children discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the esi-tech helpdesk (http://esi-tech.co.uk/helpdesk/). The school manages its own filtering service, via Sophos.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. This will include the ability to monitor and track ALL websites and URLs visited. This is done via the school's active directory of account holders to identify the member of staff, and the management tools within Sophos to identify the URL's visited and the time and length of connection, on the particular user's account.

Whilst staff who possess a school provided device, for example a staff laptop, agree to the terms of use, which include the ability of school management to monitor all activity on the device, the monitoring of websites visited will be undertaken in the following circumstances:
1. An automatic report generated by Sophos that there has been suspicious activity on a device, such as a virus being detected
2. Concerns raised by a member of staff about unsuitable sites being visited
3. Contact by the LA ICT team/Unity ICT team regarding suspicious activity
4. Police or other legal/criminal related services requesting access

Individual devices cannot be monitored, only the type of device (for example iPhone) is annotated on reports in Sophos. In addition, the devices identification number is registered, meaning that in

the cases listed above, it would be possible to trace the specific device. However this could only be done with the participation of the holder of the device.

In addition generic reports regarding holistic internet usage in school will be provided to school managers or the Local Governing Body upon request – for example to determine which websites are utilised across school for learning, determining the level of bandwidth being used and required at school. This will be reports for all devices that connect to the school's networks.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting Personal Data
Personal data will be recorded, processed transferred and made available according to the General Data Protection Register 2018 and the Trust's policy and privacy notices.

Authorising Internet Access
All staff must read and sign the Responsible Internet Use statement before using any Trust ICT resource.

Assessing Risks
The school will take reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The Trust will not accept liability for the material accessed, or any consequences of Internet access.

The Trust will audit ICT use on a regular basis to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.

Handling E-safety Complaints
Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Executive Principal.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Any illegal issues will be discussed with the police.

Staff and the E-safety policy
All staff will be informed of and have access to the school E-safety policy and its importance explained.

Staff should be aware the Internet traffic can be monitored and trace to the individual user. Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues. Staff should understand that telephone or online communications with children can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

Enlisting parents' support

Parent's attention will be drawn to the school E-safety policy in newsletters and on the school website