E-SAFETY POLICY

Dates of review:
January 2017
December 2020
October 2023

Date	Section of Policy	Amendment
October 2023	Table of changes	Table of changes added
October 2023	Related Documents	Amendment to name of ICT & Acceptable Use Policy

Delamere School E-Safety Policy

Background / Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- **Access to illegal, harmful or inappropriate images or other content**
- **Un-authorised access to / loss of / sharing of personal information**
- **The risk of being subject to grooming by those with whom they make contact on the internet.**
- **The sharing / distribution of personal images without an individual's consent or knowledge**
- **Inappropriate communication / contact with others, including strangers**
- **Cyber-bullying**
- **Access to unsuitable video / internet games**
- **The potential for excessive use which may impact on the social and emotional development and learning of the young person.**

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and safeguarding policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Development and Monitoring

Role	**Named Person**
Computing Co-ordinator & E-Safety Lead	Amy Burt
IT technicians	Infinity Computing
Designated Safeguarding Lead	Barbara Telford (Deputy Headteacher)
Senior Information Risk Officer	Sally Burston (Headteacher)

This e-safety policy has been developed by the Headteacher in conjunction with the School Leadership team and approved by the Governing Body. As part of this policy, records will be maintained of E-Safety related incidents involving staff and pupils and any incidents recorded will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.

Should serious e-safety incidents take place, the following external persons / agencies should be informed:	**Trafford Local Authority** **Police (if criminal activity has occurred)**

The school will monitor the impact of the policy using:

- **Feedback from staff, pupils, parents / carers, governors**
- **Logs of reported incidents**
- **Internet activity monitoring logs**

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

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

Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher / Senior Leaders

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Computing Co-ordinator/Designated Safeguarding Lead.
- The Headteacher is responsible for the implementation and effectiveness of this policy. She is also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- The Headteacher / Senior Leaders are responsible for ensuring that the Computing Co-ordinator/ Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles.
- The Headteacher / 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (See Managing Allegations against a member of staff policy/guidance)

Computing Co-ordinator + Designated Safeguarding Lead

The Computing Co-ordinator + Designated Safeguarding Lead:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Reports to the School Leadership Team serious breaches of the E-Safety Policies
- Provides training and advice for staff
- Liaises with the Local Authority
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

Teaching and Support Staff

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 E–Safety policy, school Staff Acceptable Use ICT Policy
- They report any suspected misuse or problem to the Computing Co-ordinator/Designated Safeguarding Lead for investigation / action / sanction
- Digital communications with pupils and parents / carers (email / voice) should be on a professional level
- Pupils understand and follow, as appropriate for age and ability, the school e-safety and acceptable use policy
- In lessons where internet use is planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Computing Co-ordinator + Designated Safeguarding Lead

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting
- Radicalisation (extreme views)
- CSE

Pupils

- Pupils at Delamere enjoy high levels of supervision due to their special educational needs & disabilities.
- Where appropriate for age and ability, children are supported by staff to understand how to use the internet responsibly and appropriately.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through their website: http://www.delamere.trafford.sch.uk/esafety-guide-for-parents/410.html

Parents and carers will be responsible for:

- Accessing the school website and keeping up to date with esafety rules.

Parents / carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

Policy Statements

Education – Pupils

E-Safety education will be provided in the following ways, as appropriate to pupils' age and ability:

- A planned e-safety programme should be provided as part of Computing/ PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of activities
- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices through a planned programme of activities
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – Parents and Carers

Many parents and carers have only a limited understanding of e-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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, web site
- Parents evenings
- Reference to external E-Safety websites
- High profile events such as Internet safety day
- Family learning opportunities

Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required

Technical – Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / 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 e-safety responsibilities:

- School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the e-safety technical requirements for Trafford Local Authority
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- Staff will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school maintains and supports the managed filtering service provided by Trafford LA. Any incidents or activities regarding filtering will be handled in accordance with their policy.
- Remote management tools are used by the managed service provider to control workstations and view users activity
- Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data
- Protection from cyber attacks - we will work with our IT support provider to make sure cyber security is given the time and resources required to make the school secure. We will provide

appropriate training to staff, including how to identify suspicious emails; how to deal with a request for bank details, personal information or login details; how to vverify requests for payments or changes to information.In liaison with our IT support provider we will implement controls to keep our systems safe and which can be regularly reviewed/tested to ensure they are as effective and secure as they can be.

- Guest access to the school network will be authorised by the School Office Team through the provision of limited access guest accounts which do not give access to personal information about pupils or staff.
- The school infrastructure and individual workstations are protected by up to date anti-virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- Good E-Safety practice is an integral part of the school Computing curriculum and will be taught to pupils as part of their ICT learning.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

Use of digital photographs and video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. More detailed guidance on the collection, handling and storage of personal data can be found in the school Data Protection Policy.

Communications

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure.
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the E-Safety Coordinator – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and parents / carers must be professional in tone and content and be via official used systems.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer.

Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The incident should be following in accordance with the safeguarding policy and if necessary, the police should also be informed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

Appendices

Guidelines for the use of communication technologies within school

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed in designated areas	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	✓							✓
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones or personal camera devices				✓				✓
Use of personal hand held devices		✓						✓
Use of personal email addresses in school during own time	✓							✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of school social networking sites	✓							✓
Use of personal blogs				✓			✓	
Use of educational blogs	✓						✓	

Related Documents

ICT & Acceptable Use Policies

Data Protection Policy

Safeguarding Policy

Anti-bullying Policy