



Templefield Lower School

E-Safety Policy

Created: March 2020

Review: March 2021

Introduction:

At Templefield we are dedicated to ensuring children are taught the skills they need to access a range of technologies at school and home safely. With recent technological advances it is even more important for children to be educated in E-Safety, especially with the access to the internet through many different devices. Our aims are to ensure:

- Children are able to use technology to support their learning at school.
- They can use a wide range of equipment safely.
- Children can use technology outside of school in a safe way, including communicating online.
- They will know what to do if they feel unsafe when using technology.
- They will know the importance of keeping their personal information.

The Law:

Our E-Safety Policy has been written following government guidelines and is part of other policies we have at school that refer to keeping children safe.

Roles and Responsibilities:

Headteacher and Computing Subject Leader

- Ensure the policy is implemented, communicated and compliance with the policy is monitored.
- Ensure staff training in e-safety is provided and updated annually as part of safeguarding training.
- Ensure immediate action is always taken if any risks or dangers are identified ie reporting of inappropriate websites.
- Ensure that all reported incidents of cyber-bullying are investigated.
- Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material.
- Ensure information is provided to parents and carers on how to keep their children safe online through newsletters and information meetings.

Teachers and Staff will:

- Keep passwords private and only use their own login details, which are stored securely.
- Monitor and supervise pupils' internet usage and use of other IT resources.
- Adhere to the Acceptable Use Agreement with a signed copy kept on file.
- Promote e-safety and teach e-safety units as part of computing curriculum.
- Engage in e-safety training.
- Only download attachments/material onto the school system if they are from a trusted source.
- When capturing images, videos or sound clips of children, only use school cameras or recording devices.

It is essential that pupils, parents/carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Governors will:

- Ensure that the school is implementing this policy effectively.
- Adhere to the acceptable use agreement when in school.
- Have due regard for the importance of e-safety in school.

Teaching and Learning:

The school will actively teach E-safety at an age-appropriate level. The school follows a scheme of work for each year group covering: what should and shouldn't be shared online, password control and cyber bullying among other topics. E-safety will also be embedded throughout learning whenever children are using ICT in other lessons.

Monitoring Safe and Secure Systems:

- Internet access is regulated by HCC supplied filtered broadband connection which blocks access to unsuitable websites.
- Antivirus software has been installed on all computers and is to be maintained and updated regularly.
- Staff passwords should be changed regularly and must be strong passwords.
- Staff take responsibility for safeguarding confidential data saved to laptops, ie use of strong passwords. If personal data has to be saved to other media, eg data sticks or CDs, it is to be encrypted or strong password protected. However, with the introduction of Google Drive this should not be needed.
- Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times.
- All teaching staff have access to their own Google Drive which allows them to store and share information electronically. This stops the need for portable storage devices as everything is stored in one place and can be accessed when needed via the internet.

Safe use of the Internet and Web Filtering:

- All staff and pupils will have access to the internet through the school's network
- All staff and volunteers must read and sign the Staff Acceptable Use Agreement.
- All children must read and sign the Pupil Acceptable Use Agreement in their classroom.
- If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Headteacher to pass to HCC
- If an adult finds a site that they consider unsuitable they should report it to the Headteacher and it can be blocked accordingly.

The use of Email:

- All teaching and support staff are provided with a school email address.
- Staff should use this address when sending work-related emails.
- All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary.
- Staff emails should never be used to forward 'chain' or 'junk' email.
- Staff should not communicate with pupils via email. Staff emails should not be displayed on the Interactive Whiteboards as this does not comply with GDPR guidelines.

The School Website:

- The school website complies with statutory DFE requirements
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted online.

Social Networking, Social Media and Personal Publishing (blogging):

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils will not access social networking sites, eg Facebook or Twitter in school. They will be taught about how to stay safe when using such sites at home. School and class blogs are run through the school website and are password protected.

Staff Private use of Social Media:

- No reference should be made in social media to students / pupils, parents / carers / school staff or issues / situations related to the school
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- Staff are not permitted to maintain a Social Media relationship with any pupil, current or alumni until such time that the pupil turns 18.

The Use of Cameras, Video and Audio Recording Equipment:

- Staff may only use the school's photographic or video devices to support school trips and curriculum activities. Photos should only be uploaded to the school system.
- They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher or Deputy Headteacher, nor circulate them in electronic form outside the school.
- It is never acceptable to use photographic or video devices in changing rooms or toilets.
- During performances for parents reminders are given to ensure that parents are not taking pictures with other children in and then sharing them on social media.

Personal Mobile Phones and Mobile Devices:

- Use of mobiles is discouraged throughout the school, particularly in certain areas. The areas which should be considered most vulnerable include: toilets and changing areas, including where children change for swimming.
- During contact with children all staff should keep their mobile phone in a safe place. Mobile phones should only be used in designated areas at designated times.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the head teacher.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Management of Online Safety Incidents:

- There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions; all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes; support is actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
 - Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
 - The Police will be contacted if one of our staff or pupils receives online communication that we consider

is particularly disturbing or breaks the law;

- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform MASH.

Working in Partnership with Parents:

Parents' attention will be drawn to the E-Safety Policy through the school newsletters, information evenings and on the school website. We want to work in partnership with parents to ensure we are doing all we can to keep children safe both in school and out. Questionnaires are used to gauge parental understanding of E-Safety and offer parent workshops to provide information on e-safety. Parents will be requested to sign an Acceptable Use Agreement as part of the Home School Agreement on entry to the school.

Protecting School Staff:

In order to protect school staff we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

Safeguarding – scope of this policy (See also Safeguarding and behaviour policies) The Education and Inspections Act 2006 empowers the Head Teacher to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the school's Behaviour Management Policy.

The school will deal with such 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.