EWELL CASTLE SCHOOL
Where Children Thrive

Whole School
(including EYFS)

E-Safety

Table of Contents

Reviewed	Summer 2023
Name of owner/author	STL
Approval by	Executive Leadership Team/Governors
Target Audience	Whole School Community/Public
Where available	Website, Staffshared Drive
Review Date	Summer 2024

1 Policy Statement

It is the duty of Ewell Castle School to ensure that every pupil and member of staff in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, radicalisation and abuse.

This policy reflects the values and philosophy of Ewell Castle School in relation to the use of ICT for teaching and learning that ensures the E-safety of pupils. It provides a framework within which all employees work. It gives guidance on planning, teaching, assessment and should be used in conjunction with each department's Schemes of Work.

2 Importance of E-Safety

The use of ICT at Ewell Castle School is primarily to enhance learning through the use of established and innovative technologies.

All forms of electronic access can promote educational excellence by facilitating resource sharing, innovation, and communication. However, for both pupils and teachers, all these forms of electronic access at School are considered a privilege and not an entitlement.

As there is the possibility that pupils may encounter inappropriate material on the Internet, the School will actively take all reasonable precautions to restrict student access to both undesirable and illegal material.

It is the responsibility of every staff member, both teaching and non-teaching, to ensure that the spirit of the policy set out below is implemented across all relevant areas of learning, teaching, administration and support.

This policy applies to all members of our School community, including those in our EYFS setting. Ewell Castle School seeks to implement this policy through adherence to the procedures outlined below.

Teachers are responsible for guiding pupils in their on-line activities, by providing clear objectives for internet use. Teaching staff will also ensure that pupils are aware of what is regarded as acceptable and responsible use of the Internet.

3 Teaching and Learning

3.1 Pupils

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression with opportunities for creative activities and will be provided in the following ways:

- E-safety is planned and explicitly taught as part of the curriculum within KS3 Computing, where content is regularly re-visited. Key E-safety messages are reinforced across all Key Stages and within all curriculum subjects as required.
- Key E-safety messages are reinforced as part of a planned programme of assemblies and tutorial/ pastoral activities, as well as through PSHE. This includes the use of external speakers.

(And Safer Internet Day)

- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Pupils are helped to understand the need for the Pupil Acceptable Use Policy agreement and encouraged to adopt safe and responsible use both within and outside the School.
- Pupils are helped to understand the benefits associated with social media, online posting and messaging.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such situation, staff can request IT support to remove those sites from the filtered list for those pupils. Any requests to do so should be audited by the IT Manager, and clear reasons for the need must be established and recorded.

3.2 Parents and Carers

Parents play an essential role in the education of their children and in the monitoring/regulation of their son or daughter's on-line behaviour. The School provides information and awareness to parents in support of this in a range of ways, including: seminars (at Information Evenings, for example), the School Bulletin, My School Portal, the School website, Twitter, newsletters and direct parental correspondence, as required.

3.3 Staff and Volunteers

It is essential that all staff who are granted access to the School network receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be arranged and overseen by the Deputy Head of the Senior School or the IT Manager, recorded as having taken place.

- Training is made available to staff and is regularly reinforced.
- All new staff receive training as part of their induction and should fully understand the ICT Acceptable Use agreement.
- The Safeguarding Leads will receive regular updates through attendance at external training.
- This policy and its updates will be presented to and discussed by staff as part of Inset training.

4 Managing Internet Access

4.1 Authorising Internet Access

- All staff must read and sign the "ICT Acceptable Use Agreement for Staff" before using any School ICT resource.
- All pupils must read and sign the "ICT Acceptable Use Agreement for Pupils" before using any School ICT resource.
- The School will maintain a current record of all staff and pupils who are granted access to School ICT systems.
- Parents will be asked to sign and return a consent form.

4.2 Information System Security

- School technical systems will be managed in ways that ensure that the School meets recommended technical requirements.
- School network system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to School technical systems and devices

- All users will be provided with a username and secure password by IT who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password at set intervals.
- Security strategies will be discussed regularly with the Senior Leadership Team ("SLT") and links with the Local Authority will be maintained.
- Internet access is filtered for all users. Illegal content is filtered by the filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored.
- The School has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the School network and users are made aware of this in the Acceptable Use Agreements
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the School systems and data. These are tested regularly. The School infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" e.g. supply teachers or visitors onto the School systems.

4.3 E-mail

- All pupils are issued with their own personal e-mail addresses for use on the School network and by remote access.
- All pupils email will be monitored for appropriateness of content.
- Pupils should immediately report to a teacher any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature.
- Staff to pupil email communication must only take place via a School email address or from within recognised School systems e.g. iSAMS or Show My Homework.
- Incoming e-mail from outside the School should be treated as suspicious and attachments opened with care.

4.4 Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and only identified in accordance with the Use of Photographic Images and Photographic Consent Form.
- Parents are clearly informed of the School policy on image taking and publishing, both on School and independent electronic repositories.

4.5 Use of School devices

- School devices assigned to a member of staff as part of their role must have a unique username and password or device lock so that unauthorised people cannot access the content. When they are not using a device, whether School or personal, staff should ensure that it is locked to prevent unauthorised access.
- School owned mobile technologies are available for pupil use and stored in locked containers. Access is available during lessons via the member of staff taking that lesson.

5 Radicalisation

Ewell Castle School values freedom of speech and the expression of beliefs or ideologies as fundamental rights underpinning British values. The School's approach to safeguarding from radicalisation can be found in the Safeguarding Policy.

Ewell Castle School understand that pupils and staff may sometimes be exposed to extremism and radicalisation through their use of ICT. The School takes guidance from the Government's

'Prevent Strategy' (2011) and from Keeping Children Safe in Education (Sept 2020), and recognises its duty of care to pupils and staff in safeguarding them from the risk of extremism and radicalisation when they are using the School's ICT facilities.

- Staff will vigilant and report any computer activity that may suggest a child is involved in radicalisation and extremism
- Pupils are regularly taught about how to stay safe when using the internet and are encouraged to recognise that people are not always who they say they are online.

6 Social Media – Protecting Professional Identity

The School has a duty of care to provide a safe learning environment for pupils and staff. The School could be held indirectly responsible for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the School liable to the injured party. Reasonable steps to prevent predictable harm must be in place. The School provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the School through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; the General Data Protection Regulation (2018); reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to pupils, parents or School staff
- 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 are regularly checked to minimise risk of loss of personal information.

Please also refer to the Staff Code of Conduct.

7 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (2018) or any UK legislation which replaces it. The School has data protection policies which include electronic data.

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against accidental loss of, or damage to, personal data. This is in relation to data belonging to all members of the School community. As such, no member of staff is permitted to remove sensitive personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Principal. Where a member of staff is permitted to download data off site it will need to be password protected.

There are two exceptions:

- iSAMs may be used on personal devices provided that the device used is secure and password protected.
- For pupils on any residential/day trips (including away fixtures), medical information and other relevant details (e.g. passport details) may be taken off site.

8 Assessing Risks

The School will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a School computer. The School cannot accept liability for the material accessed or any consequences of internet access.

The School will monitor ICT use to establish if this Policy is adequate and that the implementation of it is appropriate and effective.

9 Handling E-Safety Complaints

- Complaints of internet misuse will be dealt with by a Form Teacher or Head of Year and, if required, a senior member of staff.
- Any complaint about staff misuse must be referred to the Deputy Head of Senior School, the Head Teacher of the Preparatory School or the Principal.
- Complaints of a child protection nature must be dealt with in accordance with Safeguarding Policy.
- Pupils and parents will be informed of the Complaints Policy and procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the School's Behaviour, Rewards and Sanctions Policy.

10 Community Use of the Internet

All use of the School internet connection by community and other organisations will be in accordance with this Policy.

11 Staff and the E-Safety Policy

- All staff will be given a copy of this Policy and its importance explained.
- As part of Induction for new staff, the content of this policy will be covered. New staff will be expected to acknowledge that they have understood and agreed to work within the agreed guidelines.
- Staff should be aware that internet traffic can be monitored and traced 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.

12 Enlisting Parents' Support

- Parents' and guardians' attention will be drawn to this Policy in newsletters, the School brochure and on the School website.

- The School will ask all new parents to sign the parent /pupil agreement when they register their child with the School.
- Parents will be given E-safety training regularly with a focus on education and having an overview of tools to allow them to take control whilst not undermining trust.

13 Review and Development

13.1 Procedure

This document, together with the effectiveness of its procedures, will be reviewed annually by the Senior Management Team and Governing Body and as events or legislation change requires.

13.2 Links with other Policies

This policy should be read in conjunction with the following documents:

Anti-Bullying Policy
Behaviour for Learning Policy
Complaints Policy
Data Protection and related Policies
Pupil Acceptable Use of ICT
Safeguarding Policy
Staff Acceptable Use of ICT
Staff Code of Conduct