Mayfield	Policy Name: Online Safety Policy Owner: Deputy Head Review Date: August 2021 Next Review Date: August 2022 This policy was revised as regulations or review demands.

Definition

In an environment where the use of information technology is essential to learning and where the rapid development of new technologies and applications gives users ever increasing access to an international network of information and contacts, it is essential that we prioritise the safe use of these facilities and enable the girls in our care to be both adequately protected and to learn the necessary skills to protect themselves.

Online safety is a safeguarding issue rather than an ICT issue. All those working in the school or attending the school as a pupil have a duty to be aware of online safety at all times, to know the required procedures and to act upon them.

Duty of Care

The Designated Safeguarding Lead has overall responsibility for online safety matters. The Co-ordinator of ICT for KS3 and 4 has responsibility for the online safety curriculum for the girls throughout the school. The security of the network and IT facilities is the responsibility of the Systems Director.

All staff have a responsibility to support online safety provision through the school and to enable their pupils to use IT responsibly and safely. They also have a duty to abide by the Acceptable Use of ICT (Staff) Policy and Social Media Policy.

Girls at all stages of the school need to understand their responsibilities and liabilities in the event of deliberate attempts to breach online safety protocols (See Acceptable Use of ICT (Pupil) Policy).

It is the responsibility of the school to build a culture of trust, responsibility and the expectation of safe behaviour, along with support when problems do arise to secure the safety and wellbeing of our pupils.

Scope of Policy

Online safety concerns the day to day running of the physical network and information passing through it, whether connected via the internet or local area networks, or by access to the network via the Remote Desktop Service (RDS).

The policy emphasises the School's commitment to the teaching of safe and responsible use of ICT.

The policy links with the Acceptable Use of ICT (pupil) Policy and the Acceptable Use of ICT (Staff) Policy.

Online safety also covers technology not owned by the School. The School would respond to online safety threats involving members of the community whether they occurred during school time, on the School site or if perpetrated using equipment not owned or operated by the School.

Of particular concern are issues of unsupervised access to girls via the internet, and other networks, by adults but also possible cyberbullying between girls at the school and from other external young people, and access to inappropriate and dangerous material. This is at the heart of the School's promotion of online safety and, as safeguarding issues, are significant threats against which we need to guard.

This policy and our online safety provision are reviewed and monitored by the Designated Safeguarding Lead, in liaison with the Coordinator of ICT and the Systems Director. The policy is reviewed at least annually.

Teaching Safe Practices

Staff are regularly updated on issues of online safety and particularly the development of new technologies and applications. The ICT department offer support and training to staff on online safety issues both formally in groups and at an individual level.

New staff are made aware of our online safety processes and procedures as part of induction.

A curriculum of online safety is taught from Years 7-10 and further issues of online safety (particularly cyber-bullying and the use of social media) and the implications of technology are included in the whole School Life Skills programme and Tutor programmes.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful content.

Contact: being subjected to harmful online interaction with other users.

Conduct: personal online behaviour that increases the likelihood of or cases, harm.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

It is crucial in the promotion of online safety that we work collaboratively and supportively with parents. The School offers a range of events where parents can learn more about the issues which may impact on their families and how they can support the development of safer practices. A half-termly online safety newsletter to parents also raises awareness of issue and developments in the field.

Provision of a Safe Environment in School

The School has three levels of protective systems in place.

- The firewall protects against malware, viruses and other external attack
- The content filter system used is Lightspeed Rocket, which filters all internet access. This notifies the IT Helpdesk system when any user attempts to access inappropriate sites and material.
- Horizon View on the virtualised system provides protection on staff and pupils own devices used under the Bring Your Own Device (BYOD) system.

Mindful that the prevalence of 3G and 4G internet access on Smart phones, means that pupils can often circumvent our security systems, the emphasis on education is again key. Pupils in Years 7,8 and 9 are allowed limited access to their phones in School, and boarders up to year 10 have their phones and other devices taken in

by staff overnight. Pupils using the School Wi-Fi on their own devices are protected by our filters and so they are encouraged to do this and given support to log on to our system.

Procedures to be followed in the event of an online safety breach

All instances of online safety breach, whether identified by direct observation or disclosure, will be taken seriously.

All staff should report any suspected online safety breach as a safeguarding issue,

If the breach has been disclosed by a pupil this should be reported using MyConcern, and the member of staff should speak to the DSL as a matter of urgency.

If the breach has been directly **observed** by a member of staff, they should note the following.

- In case of an accidental breach

  Note the website concerned and the nature of the content, remove the image/content and reassure the pupil(s) involved. Complete an incident file note and inform the DSL, as well as referring the website to the IT Helpdesk immediately for urgent blocking

- In case of an intentional breach

  Note the nature of the incident and preserve any evidence (for example by taking a screen shot by pressing 'print screen' and copying into a Word document)

Complete an incident file note and inform the DSL as quickly as possible. All such incidents will be fully recorded and logged in the Welfare/Child Protection records held by the Designated Safeguarding Lead. For a very serious incident, external agencies may need to be involved in the response to the situation and the DSL will take advice from the SPOA

If a referral is necessary to SPOA (Single Point of Advice) this will also be recorded with the actions required.

Where there is danger of harm to a child the Child Protection Procedures will be followed (See Safeguarding Policy). Other relevant policies are the Anti-Bullying Policy, Rewards and Sanctions Policy, and Staff Code of Conduct and Disciplinary policy.

For more government guidance please refer to KCSIE (September 2021), Teaching online safety in school (June 2019) and Information Sharing (July 2018).

Password Policy

Passwords must not contain the user's account name or parts of the user's full name that exceed two consecutive characters.

They must be at least fourteen characters in length and contain characters from each of the three following categories:

- Roman uppercase characters (a-z)
- Roman lowercase characters (a-z)
- Numeric characters (0-9)

Both the Staff and Pupil Acceptable Use of ICT Policies make clear that users must not log on using any other username/password than their own. This is considered a serious breach of ICT security.

Staff Use of School Laptops

Teacher laptops, and all school provided equipment, must only be used by the employee of the school (NOT family members, friends etc)

Staff must take reasonable care to secure such equipment (e.g. not to be left in a car overnight, or in plain sight)

Data Transfer

The School's Data Protection Policy sets out fully how data is managed and secured.

All data is stored on site and back up discs are held in three fully secured locations on site

Staff bringing in files from home for Teaching and Learning

Staff are expected to ensure that any file they propose to use in school is free from virus/spyware/malware. The Sophos software, which is an automated virus check, on the school system is a back up to this requirement.

It is the responsibility of staff to ensure that the material contained in the file is fit for purpose and does not contain any offensive or copyright material.

Monitoring and reporting procedures

Records of any online safety breaches or significant concerns will be held by the DSL on the child's MyConcern File or Child Protection file.

These records may be shared with legitimate agencies as necessary to ensure online safety.

The online safety policy and procedures are audited each year, by the Designated Safeguarding Lead and the Nominated Governor for Safeguarding who also has responsibility for online safety, as part of the Safeguarding audit. This is reported to Governors and scrutinised by the Governance Committee. There is also a e-safety committee which is compromised of a member of the Senior Management Team, Head of ICT curriculum, Head of School IT, a governor and pupils.