The Friary School

E-SAFETYPOLICY

Introduction

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. However, the use of these new technologies can put young people at risk within and outside the school.

The purpose of this E-Safety policy is to help to ensure safe and appropriate use of these technologies.

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, including the Anti-Bullying Policy, Behaviour Policy, ICT Policy, Health and Safety Policy and Safeguarding Policy.

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

The E-Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school:

Governors

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

A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of E-Safety incident logs
- reporting to relevant Governors committees / meetings

Headteacher and 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 E-Safety Co-ordinator.

The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant

The Headteacher / Deputy Headteacher are aware of the procedures to be followed in the event of a serious E-Safety allegation being made. (See SSCB flow chart on dealing with E-Safety incidents, and relevant Local Authority HR / disciplinary procedures)

Designated Child Protection Officers

The Designated Child Protection Officers are trained in E-Safety issues and 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

It is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.

E-Safety Coordinator:

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.
- provides training and advice for staff
- receives reports of E-Safety incidents, decides how these incidents will be dealt with, and creates a log of incidents to inform future E-Safety developments
- reports regularly to Senior Leadership Team / E-Safety and ICT Strategy Group
- liaises with school ICT technical staff
- meets regularly with E-Safety Governor to discuss current issues, and review incident logs
- attends relevant meetings / committees of Governors
- liaises with the Local Authority

E-Safety & ICT Strategy Group

Members of the E-Safety and ICT Strategy Group will assist the E-Safety Coordinator with the production / review / monitoring of the school E-Safety policy / documents.

Technical Support Manager

The Technical Support Manager is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the E-Safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that the provision of E-Safety solutions for monitoring and filtering are operational and efficient
- that he / she keeps up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

The responsibilities for all teaching and support staff are:

- 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 school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction

- digital communications with students should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school E-Safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Students

The responsibilities for all students are:

- are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents and carers will be responsible for:

- encouraging adherence to the Student Acceptable Use Policy
- accessing the school website / network in accordance with the relevant school Acceptable Use Policy.

Rewards and Sanctions

Rewards and sanctions will be applied according to school policy, with particular reference to the:

- Anti-Bullying Policy
- Behaviour Policy

E-Safety awareness and pupil involvement in E-Safety awareness will be promoted through the school council, assemblies, the website and the school's social media.

Education & Training

Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in E-Safety is therefore an essential part of the school's E-Safety provision.

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. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- key E-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- a planned E-Safety programme should be provided as part of ICT and Tutor lessons and should be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school
- where students 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.
- students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet and to be aware of the potential consequences of plagiarism, particularly with respect to examination coursework.

Parents / 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.

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

- letters
- newsletters
- school website
- school social media
- information sessions

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 the school E-Safety Policy and Acceptable Use Policies

Governors

Governors should take part in E-Safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / E-Safety/ health and safety / child protection.

This may be offered in a number of ways:

- attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- participation in school training / information sessions for staff or parents

Technical - Infrastructure / Equipment, Filtering & 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 in ways that ensure that the school meets the E-Safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of school ICT systems
- 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.
- All users will be provided with a username and password.
- The “administrator” passwords for the school ICT system, used by the Technical Support Manager / IT Technicians must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- The school will never allow one user to have sole administrator access.
- Users 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 Friary utilises the market-leading internet safety solution ‘Smoothwall Visigo’ which not only filters user traffic, it also provides machine and human monitoring and provides reports on possible online safety issues directly to the E-Safety and Child Protection leads.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools are used by staff to control workstations and view user activity
- Appropriate security measures are in place 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.
- An agreed procedure is in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors) onto the school system and is supported by the AUP.

Communications Technologies

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students / Pupils		
Communication Technologies	Allowed	Allowed at certain times	Not allowed	Allowed	Allowed at certain times with permission	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 other camera devices		✓				✓
Use of hand held devices e.g. PDAs, PSPs		✓			✓	
Use of personal email addresses in school, or on school network		✓				✓
Use of school email for personal emails		✓				✓
Use of chat rooms / facilities		✓			✓	
Use of instant messaging			✓			✓
Use of social networking sites		✓				✓
Use of blogs		✓			✓	

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

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report to a member of staff 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 students or parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems.

Use of Digital & Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet.

However, staff and students 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.
There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the 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.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Permission from parents or carers will be obtained before photographs of students are published on the school website

Reviewed By	Policies & Procedures Committee	**Implementation Date**	Oct 2018	**Review Date**	Oct 2020