E-Safety Policy

Author: **Jade Driscoll, Deputy Head Teacher**
Policy Reference: **001**
Adopted by Governors: **September 2015**
Review Date: **September 2016**

Contents

Page

Executive Summary

The e-Safety policy sets out the framework and expectations that all staff, learners and Baysgarth School community should adhere to in respect to the use of computing equipment, the internet and all forms of electronic communication such as email, mobile phones, portals/intranets, social media sites and related learning technologies.
The e-Safety policy is designed to detail the principles all users should adhere to when using these services. This guidance does not attempt to cover every possible situation but should be used as a supporting framework in relation to e-Safety.

1. Introduction

Baysgarth School recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide safe and secure internet access to all learners and staff and encourage the use of ICT and learning technologies in order to enhance skills, promote achievement and enable lifelong learning and world class outcomes.

However, the accessibility and global nature of the internet and associated learning technologies that are available mean that we all need to be aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the school while supporting staff and learners to identify and manage risks safely, independently and with confidence.

We believe this can be achieved through a combination of security measures, training, guidance and the implementation of the relevant policies. In addition to our duty to safeguard staff and learners and the 'Every Child Matters' agenda, we will do all that we can to make our staff and learners e-Safe and to satisfy our wider duty of care.

OfSted Key features of good and outstanding e-Safety practice
From Ofsted's perspective, e-Safety is a critical part of the inspection process. The table below details the key features found when good or outstanding e-Safety practice is in place.

Whole school consistent approach	- All teaching and non-teaching staff can recognise and are aware of e-Safety issues. - High quality leadership and management make e-Safety a priority across all areas of Baysgarth School (the school may also have achieved a recognised standard, for example the e-Safety Mark). - A high priority given to training in e-Safety, extending expertise widely and building internal capacity. - The contribution of pupils, parents and the wider school community is valued and integrated.
Robust and integrated reporting routines	- School-based online reporting processes that are clearly understood by the whole school, allowing the pupils to report issues to nominated staff, for example SHARP. - Report Abuse buttons, for example CEOP. Clear, signposted and respected routes to key members of staff. Effective use of peer mentoring and support.

Staff	• All teaching and non-teaching staff receive regular and up-to-date training. • At least one staff member has accredited training, for example CEOP, EPICT.
Policies	• Rigorous e-Safety policies and procedures are in place, written in plain English, contributed to by the whole school, updated regularly and ratified by Governors. • The e-Safety policy should be integrated with other relevant policies such as behaviour, safeguarding and anti-bullying. • The e-Safety policy should incorporate an Acceptable Usage Policy that is signed by pupils and/or parents as well as all staff and respected by all.
Education	• A progressive curriculum that is flexible, relevant and engages pupils' interest; that is used to promote e-Safety through teaching pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. • Positive rewards are used to cultivate positive and responsible use. • Peer mentoring programmes.
Infrastructure	• Recognised Internet Service Provider or RBC together with age/maturity related filtering that is actively monitored.
Monitoring and Evaluation	• Risk assessment taken seriously and used to good effect in promoting e-Safety. • Using data effectively to assess the impact of e-Safety practice and how this informs strategy.
Management of Personal Data	• The impact level of personal data is understood and data is managed securely and in accordance with the statutory requirements of the Data Protection Act 1998.

2. Creation, Monitoring and Review

The e-Safety Policy has been prepared with guidance from DfE Principles of e-Safety, previous Baysgarth School e-Safety Policies and advice and guidance from Professional Services and school colleagues.

It is strongly recommended that an annual review of the e-Safety policy is carried out by a group in the school that includes the e-Safety officer, the Child Protection Officer, a Senior Leadership Team representative, a member of the ICT support team, learners from the pupil/student council, a teaching staff representative, a support staff representative, a parent representative, a Governor representative and a local community Police Officer.

The impact of this policy will be monitored regularly with a full review being carried out at least once a year. This policy will also be reconsidered where particular concerns are raised or where an e-Safety incident has been recorded.

3. Policy Scope

The e-Safety policy applies to all users, learners, staff and all members of Baysgarth School community who have access to the school ICT systems, both on the premises and remotely. Any user of the school ICT systems must adhere to and sign a hardcopy of the appropriate ICT Acceptable Use Agreement. The e-Safety Policy applies to all use of computing equipment (fixed and mobile), the internet and all forms of electronic communication such as email, mobile phones, portals/intranets and social media web sites.

4. Roles and Responsibilities

There are clear lines of responsibility for e-Safety within Baysgarth School. The first point of contact should be David Roberts, the e-Safety Officer. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their Line Manager and the e-Safety Officer. All teaching staff are required to adhere to this incident reporting procedure.

When informed about an e-Safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. All learners must know what to do if they have e-Safety concerns and who to talk to. In most cases, this will be the e-Safety Officer or the Child Protection Officer. Where any report of an e-Safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Child Protection Officer may be asked to intervene with appropriate additional support from external agencies.

Listed below are the roles and responsibilities that should be in place in Baysgarth School/ are referred to in the e-Safety Policy:

e-Safety Officer
The e-Safety Officer is responsible for keeping up to date with new technologies and their use, as well as attending any relevant training. The e-Safety Officer will be expected to lead the e-Safety agenda, review the e-Safety Policy, deliver staff development and training, manage the reporting procedure, record incidents, report any developments and liaise with the Senior Leadership Team and external agencies to promote e-Safety within Baysgarth School community. The e-Safety Officer may also be required to deliver workshops for parents.

Learners
Learners are responsible for using the school ICT systems, mobile devices and learning technologies in accordance with the e-Safety Policy and the Baysgarth School Student e-Safety Charter, which they must sign at the time of registration at the school. Learners must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. They are responsible for attending e-Safety lessons as part of the curriculum and are expected to know and act in line with other relevant school policies, for example; Mobile Phone Use, Sharing Images, and Cyber-Bullying. They must follow the reporting procedures where they are worried or concerned, or where they believe an e-Safety incident has taken place involving them or another member of the Baysgarth School community.

Staff

All staff are responsible for using the school ICT systems, mobile devices and learning technologies in accordance with the e-Safety Policy and the Baysgarth School Staff e-Safety Charter, which they must sign and submit to the e-Safety Officer. Staff must act safely and responsibly at all times when using the internet and/or mobile/learning technologies. Staff are responsible for attending training on e-Safety and displaying a model example to learners at all times through embedded good practice.

All digital communications with learners must be professional at all times. Online communication with learners is restricted to school provided systems. External platforms not hosted by the school, for example social media sites, may only be used where a Risk Assessment has been completed by the member of staff and submitted to the e-Safety Officer and Head Teacher for approval. If approval is granted, then the Baysgarth School Social Networking Policy must be adhered to.

All staff should adhere to the relevant school policies detailed in the e-Safety Policy and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the e-Safety Officer and/or Line Manager without delay.

5. Security

Baysgarth School will do all that it can to make sure the school ICT network and systems are safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and firewalls for servers, routers, and all school provided user devices (desktop/laptop/tablet/mobile etc.) to prevent accidental or malicious access of school systems and information.

Digital communications, including the school network, the Google Apps for Education platform, email systems, document storage and school portals/intranets may be monitored in line with the Baysgarth Data Protection Policies.

It is recommended for security purposes that all user account passwords be changed on a 45-60 day cycle where practicably possible.

6. Risk Assessment

In making use of new technologies and external online platforms, all staff must first carry out a Risk Assessment for e-Safety. This consists of a series of questions for the requestor to answer as well as a section in which they can record any relevant comments or evidence. A Risk Assessment must also be carried out where a learner is learning off site e.g. on work placement. All forms must be submitted to the e-Safety Officer for their consideration and approval.

7. Behaviour

Online communication can take many forms, whether it is by email, text, webcam or instant chat. It is essential that all staff and learners are aware of the school policies that refer to acceptable behaviours when communicating online.

- The school will ensure that all users of technologies sign and adhere to the standard of behaviours set out in the Baysgarth School Staff e-Safety Charter and the

Baysgarth School Student e-Safety Charter.
- The school will not tolerate any abuse of its ICT network, infrastructure or cloud based systems, whether offline or online. All communications by staff and learners should be courteous and respectful at all times.
- Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes.

Where conduct is found to be unacceptable, Baysgarth School will deal with the matter internally. Where conduct is considered to be illegal, the school will report the matter to the Police and other relevant external organisations as required/instructed.

8. Communications

Baysgarth School requires all users of ICT to adhere to the appropriate e-Safety Policy, which states clearly when email, mobile phones, social media sites, games consoles, chatrooms, video conferencing and web cameras may or may not be used during the school day. Any required change or extension to these policies will require the permission of the Head Teacher, with advice provided by the e-Safety Officer.

9. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

All staff and learners should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites.

10. Personal Information

Personal information is information about a particular living person. Baysgarth School collects and stores the personal information of staff and learners regularly, e.g. names, dates of birth, email addresses, assessed materials and so on. Baysgarth School will keep that information safe and secure and will not pass it onto anyone else without the express consent of the individual or learners' Parent or Carer, as appropriate.

No personal information can be posted to the school website unless it is in line with the Baysgarth Data Protection Policies. Only names and work email addresses of staff will appear on the school website and no learner's personal information will be available on the website without consent and compliance with the Baysgarth Data Protection Policies.

Staff must keep learner's personal information safe and secure at all times. When using any online or cloud platforms, all personal information must be password protected. No personal information of individuals is permitted off-site, unless the member of staff has the written consent from that individual and the written permission of the Head Teacher.

Every user accessing the school ICT systems and services, both onsite or remotely, is required to log off on completion of any activity, or where they are physically absent from a device for any period. All school mobile devices such as a laptops, USB drives, tablets or mobile devices are required to be encrypted, password protected and signed out by the e-

Safety Officer or a member of the ICT staff before leaving the premises. Where any personal data is no longer required, it must be securely deleted in line with the Baysgarth Data Protection Policies.

11. Education and Training

With the current unlimited nature of internet access, it is impossible for Baysgarth School to eliminate all risks for staff and learners. It is our view therefore, that Baysgarth School will support staff and learners to stay e-Safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For learners
Learners will attend e-Safety lessons with the first of these will taking place at the beginning of each new academic year, with follow up lessons carried out via the curriculum. Issues associated with e-Safety apply across the curriculum and learners will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.

Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. A link to the school e-Safety Policy will be available on the school network and with the rules highlighted in posters and leaflets around ICT areas and classrooms. Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

For staff
Staff will take part in mandatory e-Safety training. This will be led by the e-Safety Officer. Further resources and useful guidance and information will be issued to all staff following the session. Each member of staff must record the date of the training attended on their CPD calendar/log.

12. Incidents and Response

Where an e-Safety incident is reported to Baysgarth School this matter will be dealt with very seriously. The school will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor/teacher or to the school e-Safety Officer.

Where a member of staff wishes to report an incident, they must contact their Line Manager as soon as possible. Following any incident, the school will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place; external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. This is in line with the Baysgarth School Staff e-Safety Charter.

Serious incidents will be dealt with by Senior Management, in consultation with appropriate external agencies.

Signed: _____ **Chair of Governors**	**Signed:** _____ **Head Teacher**
Date: _____	**Date:** _____