E-Safety Policy

Written by	Adopted by Governing Body	Review Date
Mrs Hannah Burnham	Summer 2026	Summer 2028

Contents

Page

1.	Introduction	3
2.	Aim	3
3.	Policy Scope	3
4.	Roles and Responsibilities	3
5.	Security	5
6.	Behaviour	5
7.	Communications	5
8.	Use of Images and Video	5
9.	Personal Information	5
10.	Education and Training	6
11.	Incidents and Response	6

1. Introduction

The Riverview Federation recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide safe and secure internet access to all students 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 students 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 students and the 'Every Child Matters' agenda, we will do all that we can to make our staff and students are e-Safe and to satisfy our wider duty of care.

2. Aims

The aims of this policy are:

- to ensure that all teaching and non-teaching staff are aware of their roles and responsibilities with regard to e-Safety.
- to protect staff and students from adverse consequences of electronic media.
- to minimise the risks posed by the use of the internet and electronic media.

Executive Summary

The e-Safety policy sets out the framework and expectations that all staff and students of the Federation should adhere to in respect to the use of computing equipment, the internet and all forms of electronic communication including 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.

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.

3. Policy Scope

The e-Safety policy applies to all users, students, staff and all members of the Federation, 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 including email, mobile phones, portals/intranets and social media web sites.

4. Roles and Responsibilities

There are clear lines of responsibility for e-Safety within the Federation.

The first point of contact should be **David Roberts, the e-Safety Officer (Baysgarth)** or **Linda Honess (Castledyke)**

All staff are responsible for ensuring the safety of students 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 students 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 are in place in Federation:

e-Safety Officer
The e-Safety Officer is responsible for:

- keeping up to date with new technologies and their use.
- attending any relevant training and leading the e-Safety agenda.
- review the e-Safety Policy.
- Evaluate the e-safety provision within the curriculum.
- 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 the Federation.
- deliver workshops for parents.

Students
Students are responsible for:

- using the school ICT systems and learning technologies in accordance with the e-Safety Policy
- acting safely and responsibly at all times when using the internet and/or learning technologies.
- attending e-Safety lessons as part of the curriculum.
- Being aware and acting in line with other relevant school policies, for example; Mobile Phone Use, Sharing Images, and Cyber-Bullying.
- following 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 Federation.

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 Staff Acceptable Usage Policy, which they must sign and submit to the e-Safety Officer.
- acting safely and responsibly at all times when using the internet and learning technologies.
- attending and completing universal training on e-Safety.
- displaying a model example to students at all times through embedded good practice.
- Maintaining that all digital communications with students are professional at all times.
- ensuring that online communication with students is restricted to school provided systems.
- ensuring that any external platforms not hosted by the school, for example social media sites, have a Risk Assessment completed and submitted to the e-Safety Officer and Head Teacher for approval. If approval is granted, then the Social Networking Policy must be adhered to.
- adhering 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.

Parents
Parents are responsible for:

- ensuring that their child/children act safely and responsibly at home when using the internet and/or mobile/learning technologies.
- being aware and acting in line with other relevant school policies, for example; Mobile Phone Use, Sharing Images, and Cyber-Bullying.
- displaying a model example to their child/children in the home environment.
- reporting to the school where they are worried or concerned, or where they believe an e-Safety incident has taken place involving their child/children or another member of the Federation.

5. Security

The Riverview Federation 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 Federation 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. Students are reminded of this in e-safety lessons and staff in briefing notes each half term.

Staff Google accounts are protected with 2-Step verification to protect sensitive student information.

6. Behaviour

Online communication can take many forms, whether it is by email, text, webcam or instant chat. It is essential that all staff and students are aware of the behaviour policy which covers their online behaviour and Acceptable Usage Policy that refer to acceptable behaviours when communicating online.

The Federation will ensure that all users of technologies sign and adhere to the standard of behaviours set out in the Staff Acceptable Usage Policy.

7. Communications

The Federation requires all staff users of ICT to adhere to the Acceptable Usage Policy, Staff Code of Code of Conduct and Social Media Policy, which state the acceptable usage of new technologies and media for the means of communication. Any required change or extension to these policies will require the permission of the Head Teacher, with advice provided by the e-Safety Officer.

8. 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), and in line with the AI policy. This will include images downloaded from the internet and those belonging to staff or students.

All staff and students 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.

9. Personal Information

Personal information is information about a particular living person. The Riverview Federation collects and stores the personal information of staff and students regularly, e.g. names, dates of birth, email addresses, assessed materials and so on. The Riverview Federation will keep that information safe and secure in line with the Data Protection Policy and will not pass it onto anyone else without the express consent of the individual or students' Parent or Carer, as appropriate.

No personal information can be posted to the school website unless it is in line with the 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 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 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 Data Protection Policies.

10. Education and Training

With the current unlimited nature of internet access, it is impossible for the Federation to eliminate all risks for staff and students. It is our view therefore, that the Federation will support staff and students 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 Students
Students will attend e-Safety lessons with the first of these 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 students will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.

Students 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 website. Within classes, students 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.

11. Incidents and Response

Incidents involving students

Where a member of staff wishes to report an incident involving a student, they should make a referral using CPOMS.

Where an e-Safety incident involving a student is reported to a Riverview setting this matter will be dealt with following the School's Behaviour Policy.

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.

Incidents involving staff members

Where a member of staff wishes to report an incident involving another staff member, they should follow the Federation's Whistleblowing Policy.

Following any incident, the school will review what has happened and decide on the most appropriate

The e-Safety policy will be reviewed each year by the nominated member of the Senior Leadership Team and the Governing Body.

The impact of this policy will be monitored regularly with a full review being carried out at once a year.

This policy will also be evaluated where particular concerns are raised or where an e-Safety incident has been recorded.