BALLARD

BESPOKE EDUCATION

E-SAFETY AND DATA PROTECTION POLICY	
Reviewed by:	**Richard Hastings – Director of IT**
Next Review due:	**September 2024**
Next Review due:	**September 2025**

BALLARD

BESPOKE EDUCATION

E-Safety and Data Protection Policy

INTRODUCTION

This policy applies to all members of the School community, including staff, pupils, parents and visitors, who have access to and are users of the School IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, supply staff and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the School, including occasional volunteers.

Digital technologies have become integral to the lives of children and young people, both within the School and outside School. These technologies are powerful and open up new opportunities for everyone. These technologies are fantastic tools for learning and communication that can be used in School to enhance the curriculum, challenge pupils, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that pupils, staff and parents use it appropriately and practice good E-Safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

This policy aims to be an aid in regulating ICT activity in School and provide a good understanding of appropriate ICT use that members of the School community can use as a reference for their conduct online outside of school hours. E-Safety is a whole-school issue and responsibility.

The School will not tolerate cyberbullying against either pupils or staff. This will be treated as seriously as any other type of bullying and will be managed through our Anti-Bullying Policy and procedures

1. Roles and responsibility

The Head and Governors will ensure that the E-Safety and Data Protection Policy is implemented and compliance with the policy monitored but the day-to-day management of E-Safety in the School is the responsibility of the Designated Safeguard Lead (DSL) with aspects managed by the Data Protection Officer (DPO) and Director of IT. They will work closely with the Head of PSHE and Head of IT and senior pastoral and academic staff.

2. Communicating School policy

All staff are required to confirm they have read the E-Safety policy prior to starting, and this policy is available on the School's SharePoint. E-Safety guidelines are displayed around the School. E-Safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, as well as being specifically addressed in the PSHE curriculum. Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial activities and ICT lessons.

The School is aware and mindful of the non-statutory government guidance document Teaching online safety in school (2019) for maintained schools, and makes use of the recommended framework Education for a Connected World (2020) when formulating its PSHE and E-Safety programmes.

On joining the School, new pupils are required to agree to the Pupil Code of Conduct and for ICT and staff are directed towards the Staff Handbook which they are expected to adhere to.

3. Making use of ICT and the Internet in School

Using ICT and the Internet in School brings many benefits to pupils, staff and parents. The Internet is used in School to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave School.

In common with other media such as magazines and books some material available via the Internet is unsuitable for pupils. The School will take all reasonable precautions to ensure that users access only appropriate material.

Internet access is filtered for all users to help keep children safe. Different levels of filtering are used for appropriate age groups within school.

However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer or device connected to the school network. The School cannot accept liability for the material accessed, or any consequences of Internet access

Expectations of use of school computers apply to staff and pupils, both in and out of lessons.

4. Learning to evaluate internet content

With so much information available online, it is important that pupils and staff learn how to evaluate Internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read and shown how to validate information before accepting it as accurate.
- to acknowledge the source of information used and to respect copyright. The School will take any intentional acts of plagiarism very seriously.

If staff or pupils discover unsuitable sites then they are encouraged to report this to the IT Support team. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies via the IT Department or a member of the Leadership Team. Regular checks will take place to ensure that filtering services are working effectively and are in line with KCSIE.

5. Managing information systems and Data Protection

Every school is required, as part of its operation, to process a wide range of personal data. We will only process personal data about a pupil, a parent, a legal or educational guardian and staff if relevant consent has been given and/or the processing is necessary.

- The School is responsible for reviewing and managing the security of the computers and networks this data is stored on. The aim of this is to ensure that we do all that is reasonable to comply with the

law when we process relevant personal data about current, past or prospective pupils, their families and guardians and school staff. "Processing" may include creating, obtaining, recording, and holding, disclosing, amending, destroying or otherwise using personal data. To ensure this data is safe we must make sure the school's network, is safe, as far as is practicably possible, against viruses, hackers and other external and internal security threats.

The security of the school information systems and users will be reviewed regularly by the IT Support team, led by the Director of IT, and virus and malware protection software will be updated regularly. Some safeguards that the School takes to secure our computer systems are as follows:

- The School makes sure that unapproved software is not downloaded and run on any school computers. Files held on the school network are regularly checked for viruses.
- All users are provided with a username and secure password by IT Support who keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password and may be required to change this on request.
- Portable media containing School data or programmes will not be taken off-site without specific permission from the DPO. Personal data must not be sent over the Internet or taken off the School site unless safely encrypted or otherwise secured.

Individuals also have a right of access to their personal data unless an exemption applies. An individual wishing to access their personal data should put their request in writing to the DPO. We will respond to a request for access to records within forty days of receiving the request, or earlier if possible.

6. Emails and Digital communication

The School uses email and other digital communications internally for staff and pupils, and externally for contacting parents, and this is an essential part of School communication.

Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

The School has the right to monitor emails/chats/communications and their contents but will only do so if there is suspicion of inappropriate use.

Pupils should be aware of the following when using email in School, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- All pupils are provided with a school email account and pupils may only use approved email accounts on the school system.
- Pupils are warned not to reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases will be restricted.
- Pupils should immediately inform a member of staff if they receive any offensive, threatening or unsuitable communications either from within the School or from an external account. They should not attempt to deal with this themselves.

7. Published content and the School website

The School website is viewed as a useful tool for communicating our School ethos and practice to the wider community. It is also a valuable resource for parents, pupils and staff for keeping up-to-date with school

news and events, celebrating whole-school achievements, personal achievements and promoting school projects.

The website is in the public domain and can be viewed by anybody online. A team of staff, under the leadership of the Head of Marketing and Admissions, are responsible for publishing and maintaining the content of the School website.

Pupils should not publish anything on the Internet involving the School unless permission has been granted. Likewise, staff should exercise care when publishing material online to ensure that it does not bring the School into disrepute.

(i) Policy and guidance of safe use of children's photographs and work

Photographs, video and pupils' work bring our School to life, showcase our pupils' talents, and add interest to publications, both online and in print, that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

For information about how the School handles the use of images of children, please see the School's Privacy Policy

(ii) Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online.

Social media sites have many benefits, however both staff and pupils should be aware of how they present themselves online. Pupils are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The School follows general rules on the use of social media and social networking sites in School:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. Pupils are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the School's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be checked by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Any public facing blogs/websites created by pupils/year groups/school clubs as part of the school curriculum will be moderated by a member of staff, and need to be authorised in advance by the Assistant Head (Academic) and the Director of IT.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and pupils to remember that they are representing the School at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the Staff ICT Code of Conduct and AUP.
- Staff are advised not to accept friend requests from former pupils, however, if these are accepted they should understand the potential risks they put themselves in.

8. Mobile phones and personal devices

Mobile phones and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety.

- Mobile phones are not permitted up to Year 6. If a pupil in these year groups must have a phone for such reasons as transport home, the phone must be given to the Head of Section or stored in a Yondr pouch during the School day.
- Years 6 to 11 pupils can have a mobile phone in school time if they wish. If brought into School, they must be locked in a Yondr pouch or given to the Head of Section. They should be always switched off during the school day. If misused in any way they will be confiscated and lodged with the appropriate Head of Section until the end of the day**.** The following sanctions will be applied:

    - Automatic Headmaster Detention 5.00pm - 6.00pm
    - Phone to be handed in to Head of Section every day for 2 weeks

The School's expectation is that when given the opportunity, mobile devices will be used responsibly at all times and certain measures are taken to ensure that pupils adhere to this expectation. Some of these are outlined below.

- Mobile phones/devices can be confiscated by a member of staff, and the device can be searched by nominated senior members of staff if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Pupils are strongly advised not to bring mobile phones into School.
- Pupils must ensure that files stored do not contain violent or pornographic images or other material that is likely to cause offence. In very serious cases the police may be contacted.
- In an emergency, parents/guardians should phone the School, not attempt to contact the pupil directly via their mobile phone or pupil email
- The use of mobile phones by pupils on school trips is at the discretion of the trip leader.

It should be noted that power supplies for these devices must not be brought to School, as all electrical devices used in the School must be PAT tested.

(i) Mobile phone or personal device misuse

For all mobile technologies, filtering will be applied to the Internet connection when using the School Wi-Fi network and attempts to bypass this are not permitted. Any attempt to circumvent the School's security will be dealt with in the same way as any other behaviour incident. Video, audio and photographic recording must not take place by pupils without the consent of pupil(s) and teacher(s). Consent must be explicit, not implied.

Pupils

Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the School's Pastoral Care, Behaviour and Discipline Policy. Their mobile phone or device may be confiscated. In the event of confiscation, the member of staff will make arrangements for its return, which would normally be at the end of the School day.

Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that examination.

Staff

- Staff are strongly advised not to use their own personal devices to contact pupils or parents either in or out of school time.
- The School expects staff to lead by example. Personal mobile phones should be switched off or on silent during school hours.
- Any breach of school policy may result in disciplinary action against that member of staff.

- It is understood that staff may need to check text messages and/or personal messages at times during the School day. This use must not interfere with their work commitments. Staff should set an example and never use their own mobile telephones for personal reasons whilst on cover, teaching or on duty – staff should try, **when at all possible and using their professional judgement**, to use their mobiles only in staff communal areas or offices, out of the sight of pupils.

1:1 Device Schemes

In the Upper Prep and Senior School 1:1 devices are extensively used within lessons

- Pupils are expected to have their devices in all classes and fully charged at home ready for the day with a full battery. Inappropriate use of devices will be dealt with through the School's normal disciplinary procedures.
- In all classes pupils must meet their teachers' expectations in line with the Pupil Charter.
- Social media and messaging are not to be accessed during class time unless as part of a directed teaching activity.
- Pupils should be informed that devices are filtered and monitored 24/7. However, monitoring outside of school hours is not actively conducted by staff unless there is a serious safeguarding concern.

9. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the School. Information about specific strategies to prevent and tackle bullying are set out in the School's Anti-Bullying Policy. The anonymity that can come with using the Internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

More information can be accessed from non-statutory Department of Education advice: Cyberbullying:

Advice for headteachers and school staff (2014) and Advice for parents and carers on cyberbullying (2014).

Richard Hastings
Director of IT
September 2024

Policy Log:
January 2021 updated
January 2022 updated
September 2023 updated