The Bawburgh School

Online Safety Policy

Approved by:	Governors of The Bawburgh School	Date: 22/06/2023
Last reviewed on:	June 2023	
Next review due by:	July 2024	

Online Safety Policy

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

- Ofsted inspectors will always make a written judgement under leadership and management about whether or not the arrangements for safeguarding children and learners are effective.
- The school will identify a member of staff who has an overview of Online Safety, this would usually be the Designated Safeguarding Lead alongside the ICT/Computing Curriculum Lead.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior leadership and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually

Contents

Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at The Bawburgh School with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content
Exposure to inappropriate content
Lifestyle websites promoting harmful behaviours
Hate content
Content validation: how to check authenticity and accuracy of online content

Contact
Grooming (sexual exploitation, radicalisation etc.)
Online bullying in all forms
Social or commercial identity theft, including passwords
Conduct
Aggressive behaviours (bullying)
Privacy issues, including disclosure of personal information
Digital footprint and online reputation
Health and well-being (amount of time spent online, gambling, body image)
Sexting
Copyright (little care or consideration for intellectual property and ownership)
Commerce
Risks such as online gambling
Inappropriate advertising
Phishing
Financial scams

Scope

This policy applies to all members of The Bawburgh School community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of The Bawburgh School's technologies, both in and out of the school.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and staffroom
- Policy to be part of school induction pack for new staff, including information and guidance where appropriate
- All staff must read and sign the 'Staff ICT Acceptable Use' before using any school technology resource
- Regular updates and training on online safety for all staff, including any revisions to the policy
- ICT Safety Code discussed with staff and pupils at the start of each year
- ICT Safety Code to be issued to whole school community in the Autumn Term
- National Online Safety Day (February each year) will be embraced for the whole school community alongside ongoing regular input on online safety responding to the changes in developing technology.

Handling Concerns

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)
- Staff and pupils are given information about infringements in use and possible sanctions
- The Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors.

Review and Monitoring

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy, Life Skills, Computing/ICT policy).

- The online safety policy will be reviewed annually **or** when any significant changes occur with regard to the technologies in use within the school.
- There is widespread ownership of the policy and it has been agreed by the Senior Leadership Team (SLT) and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Pupil online safety curriculum

This school:

- has a clear online safety education programme as part of the Computing curriculum and PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience
- will remind students about their responsibilities through the pupil ICT Safety Code
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights

Staff and governor training

This school:

- makes regular up to date training available to staff on online safety issues and the school's online safety education programme
- provides, as part of the induction process, all staff [including those on university/college placement and work experience] with information, guidance and training on the Online Safety Policy and associated documents

This school:

- provides information for parents/carers for online safety on the school website
- parents/carers are issued with up to date guidance on an annual basis

Incident management

In this school:

- there is strict monitoring and application of the online safety policy, including the ICT Safety Code and a differentiated and appropriate range of sanctions
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Police, Internet Watch Foundation) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible
- The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA

Managing IT and Communication System

Internet access, security and filtering

In this school we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision**.**

The internet is a valuable resource for teaching and learning and is used regularly in schools and academies. However, it can also present a high level of risk if it is abused or if safe practices are not adopted.
The Bawburgh School has advised employees not to use school equipment to access the internet for private purposes unless they have permission from the Headteacher.

Employees should be made aware that the network and inappropriate use of the internet is closely monitored and individual usage can be traced. Inappropriate use of these facilities may constitute a criminal or disciplinary offence.
If employees or managers are unsure of what they can and cannot do they can seek advice from the Online Safety Helpline email: helpline@saferinternet.org.uk or call 0844 3814772.

E-mail

The school provides staff with an email account for their professional use, e.g. nsix.org.uk and makes clear personal email should be through a separate account.
We use anonymous e-mail addresses, for example head@, office@

The school will:

- contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- ensure that email accounts are maintained and up to date
- use school provisioned pupil email accounts that can be audited
- Teach the children about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The school website complies with statutory DfE requirements
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website·

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- The use of any school approved social networking will adhere to ICT Safety Code

Pupils

- are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work
- Students are required to sign and follow our Pupil ICT Acceptable use

Parents/Carers

- Parents/carers are reminded about social networking risks and protocols through our parental ICT Safety information and additional communications materials when required

Data Security

Management Information System access and data transfer

We follow the guidance from the Information Commissioner's Office to ensure that we comply with our responsibilities to information rights in school.

Digital images and video

In this school:

- we gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school (or annually)

- we do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- staff sign the school's ICT Acceptable use policy and this includes a clause on the use of personal mobile phones/personal equipment
- specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use.