Acceptable Use and E-Safety Policy

Contents

This guidance should be read in conjunction with the Data Protection Policy that outlines the school's approach relating to the collection, processing and storage of personal data; including that which is received and/or stored digitally.

This document must be reviewed at the same time as the data protection policy to ensure consistency.

1. Aims

Bournemouth School aims to:

- have robust processes in place to deliver an effective approach to ensure the online safety of students, staff, governors and volunteers, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'), by providing a working environment that encourages access to knowledge and sharing of information
- establish clear mechanisms to identify, intervene and escalate an incident where appropriate
- maintain ICT facilities for academic and administrative purposes which provide access to its community for local, national and international sources of information
- ensure that ICT facilities will be used by members of its community with respect for the public trust through which they have been provided, and in accordance with prevailing laws and such regulations and policies established from time to time by the school and other bodies
- ensure that any data held by the school is stored securely and establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

This policy applies to all staff, students, governors, contractors, consultants, authorised guests and other personnel at Bournemouth School and includes Acceptable Use, Personal Use and Prohibited Use of the school's ICT facilities, which encompass (but are not restricted to):

- network infrastructure, including (but not exclusively) the physical infrastructure whether cable or wireless, together with network servers, firewall, connections, switches and routers
- network services, including (but not exclusively) internet access, web services, email, wireless, messaging, telephony and fax services
- computing hardware, both fixed and portable, including (but not exclusively) personal computers, workstations, laptops, PDAs, servers, printers, scanners, disc drives, monitors, keyboards, tablets and pointing devices, mobile phones and electronic devices
- software and databases, including (but not exclusively) applications and information systems, virtual learning and video-conferencing environments, language laboratories, software tools, information services, electronic journals & eBooks

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, UK Council for Child Internet Safety (UKCIS), and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

Monitoring may take place periodically within the guidelines set down by the Regulation of Investigatory Powers Act (RIPA) 2000. The School retains the right under RIPA 2000 to access all information held on its information and communications facilities to monitor or intercept any system logs, web pages, email messages, network account or any other data on any computer system owned by the School. This will be for the purposes of preventing, detecting or investigating crime or misuse, ascertaining compliance with regulatory standards and School policies and to secure effective system operation.

It is a criminal offence under the Computer Misuse Act 1990 to gain unauthorised access to a computer system to make any unauthorised modification of computer material (including the introduction of a computer virus) or to interfere with any computing system provided in the interests of health and safety.

The Copyright, Design and Patents Act 1988 is applicable to all types of creations, including text, graphics and sounds, by an author or artist. This will include any that are accessible through the School's computer systems. Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of her/his rights. Users must not make, transmit or store an electronic copy of copyright material on the School's computing services without the permission of the owner.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use agreement of the school's ICT systems and the internet (Appendix I)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL's are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the headteacher, compliance manager and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents and make sure the appropriate systems and processes are in place
- Ensuring that any online safety incidents including incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy and this policy
- Working with the headteacher and ICT manager in updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (Appendix I), and ensuring that students follow the school's terms on acceptable use agreement (Appendix H)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use agreement of the school's ICT systems and internet (Appendix H)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre

- Hot topics - Childnet International
- Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix I).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum including Relationships and sex education and health education.

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including imprisonment
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

We will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

We recognise that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to bully students in line with our school behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should arrange with the compliance manager to carry out a data protection impact assessment to enable risks to be assessed where new AI tools are to be used by the school.

7. Prevention, Detection and Investigation of Misuse

The School reserves the right to inspect and validate any items of School owned computer equipment connected to the network. Any other computer equipment connected to the School's network can be removed if it is deemed to be interfering with the operation of the network.

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the headteacher / DSL
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, the staff member in conjunction with the DSL or other member of the senior leadership team will take swift and effective action within existing disciplinary and/or legislative frameworks against anyone found to be intentionally misusing the information and communications facilities. In all cases where there is the potential for the School's ICT facilities to be misused, it is the School's policy to:

- record the identity of the individual using the specific facility at any given time
- retain records as evidence (of a criminal offence or a breach of school discipline) for not less than three calendar months and make them available to those senior managers appointed by the School to investigate complaints of misuse
- report it to the police (if required)

- destroy these records after twelve calendar months unless required in connection with a specific investigation.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

Confiscate the device and report the incident to the DSL or member of SLT immediately, who will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with

- the DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Child Protections and Safeguarding Policy, and Behaviour Policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable Use

The School's ICT facilities are provided in support of teaching, learning, research, and administrative activities. All staff, students, governors, volunteers and parents are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet, see Appendix H and Appendix I. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by staff, students, governors, volunteers and visitors (where relevant) to ensure they comply with the above.

It is expected that all users:

- are registered (i.e. hold valid Bournemouth School usernames and passwords) or have been given permission by the designated authority to use the School's ICT facilities
- respect the published times of access to the facilities
- respect the rights of others, and conduct themselves in a quiet orderly manner when using the open access facilities
- comply with all valid regulations and legislation covering the use of Copyright and licensed material, including software, whether those regulations are made by law, or the originator of the material, or the distributor of the material or the School, or by any other legitimate authority
- make all reasonable efforts to send data that is 'Virus Free', and to protect themselves from viruses and hacking attempts when connected to the School's network either on or off Campus. The School will not be held responsible for any damage to user's systems or information that occurs through such virus or hacking attacks
- conform to all other appropriate policies and guidelines (including those relating to the use of the internet and e-mail – Appendices A and B)

8.1 Personal Use

The School accepts that a user's personal use of the School's facilities is within the scope of Acceptable Use, subject to the provisos within this document. It is the policy of the School:

- that provided that personal use is occasional and reasonable and does not interfere with nor detract from an individual's everyday workload and commitments, nor with the effective functioning of the School or any part of it, and that it complies with all other terms of this Acceptable Use Policy, then it will normally be tolerated
- to reserve the right to withdraw access to ICT facilities for this category of use at any time
- usage is compliant with the Data Protection Policy requirements within this document

8.2 Unacceptable Use

It is the policy of the School to prohibit the use of its ICT facilities when used or attempted to be used intentionally in contravention of the general principles of Acceptable Use. Any breach of the Acceptable Use Agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may also result in the confiscation of their own device if used inappropriately. The activities prohibited under this policy include (but are not restricted to) those listed below.

Users must not:

- cause the good name & reputation of the School or any part of it to be damaged or undermined
- create or transmit any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material
- access, create, change, store, download or transmit material which the School may deem to be threatening, defamatory, abusive, indecent, obscene, racist or otherwise offensive
- place links to websites which have links to or display pornographic and inappropriate material, facilitate illegal or improper use, or to bulletin board links which are likely to publish defamatory materials or discriminatory statements, or copyright protected works
- generate excessive noise, cause annoyance, inconvenience or needless anxiety to, or to violate the privacy of, anyone else
- allow the ICT facilities to be damaged or contaminated by food, drink or smoking materials
- interfere with the legitimate use by others of the ICT facilities, or interfere with or remove computer printout or media belonging to others
- send unwanted email, chain letters, hoax virus warnings, pyramid letters or similar schemes using the Schools email system
- falsify emails to make them appear to have been originated from someone else
- make use or possess, distribute, sell, hire or otherwise deal with any unauthorised copies of computer software for any purpose without the license of its owner
- install any software that is not licensed to the School and/or install, without authorisation, software licensed to the School on any of the School's computer systems under any circumstances
- transmit unsolicited, unauthorised, commercial or advertising material
- use the ICT facilities for commercial, social or group distribution activities unless permission has been formally granted by the Headmaster
- gain unauthorised personal commercial benefit
- gain unauthorised access to facilities or services via the School network

- allow others to gain such unauthorised access either willfully, by disclosing user names or passwords or, neglectfully, by failing to log out of the system, thereby permitting unauthorised use of a School account
- disseminate any material which may incite or encourage others to carry out unauthorised access to or unauthorised modification of the School's or others' computer facilities or materials
- introduce and transmit material (including, but not restricted to, computer viruses, Trojan horses and worms) designed to be destructive to the correct functioning of computer systems, software, networks and data storage, or attempt to circumvent any precautions taken to prevent this
- attempt to circumvent the School's firewall systems, or use file-sharing systems
- change, damage, dismantle, corrupt, or destroy (or cause to be changed, damaged, dismantled, corrupted or destroyed) any network component, equipment, software or data, or its functions or settings, which is the property of the School, staff, students, visitors, or anyone else, without the express permission of the Headmaster
- cause any of the Schools ICT services to be overloaded, impaired, disrupted, curtailed or denied (other than in compliance with the direct instruction of the Headmaster)
- connect any non-approved computer network equipment (including wireless access points) to the School network without first gaining the written permission of the Headmaster
- set up any network services (e.g. web-servers, email services, etc.) unless formally sanctioned by the Headmaster
- register any domain name which includes the name of the School or any name which may mislead the public into believing that the domain name refers to the School
- use equipment (including mains leads) which has not first been PAT Safety Tested (Portable Application Tested) by School approved staff; the equipment must display an up to date PAT label
- continue to use any item of networked hardware or software after the School has requested that use ceases because of its causing disruption to the correct functioning of the School ICT facilities, or for any other instance of Unacceptable Use
- fail to comply with any action directed by Network Manager to prevent or respond to any threats to the correct functioning of the School's ICT facilities
- contravene the local rules for School ICT facilities outside the School
- create or transmit material that infringes the copyright of another person or institution, or infringe the Copyright laws of the UK and other countries
- interfere with the legitimate activities of other users covered within the principles outlined above
- otherwise act against the aims and purposes of the School as specified in its rules, regulations, policies, and procedures adopted from time to time
- contravene applicable laws and prevailing regulations and policies applied by bodies external to the School

This policy is supplemented by guidance on the use of e-mail and the internet (Appendices A and B). Student and staff users of the School's ICT facilities are expected to sign the Acceptable Use Agreement which summarise their respective responsibilities (Appendices C and D). Best Practice guidance for users is included in Appendix E.

Guidance for students, including the use of mobile phones in school, is displayed at relevant locations around the school (Appendices F and G). Any use of mobile phones in school by students must be in line with the Acceptable Use Agreement (Appendix H).

It is essential that where ICT facilities (as listed above) are used they are used in accordance with this policy.

9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix I.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

10. Sanctions

Where misuse of ICT facilities has been identified, the matter will be investigated in accordance with the School's appropriate disciplinary procedure. Any misuse which is in contravention of the law and/or which involves the intentional access, creation, storage or transmission of material which may be considered indecent or obscene will be regarded as an act of gross misconduct.

Students may be excluded for gross misconduct under the School's student disciplinary procedures and staff may be dismissed under the School's staff disciplinary procedures. Where there is evidence of a criminal offence, the issue will be reported to the Police for them to take action. The School will co-operate with the Police and other appropriate external agencies in the investigation of alleged offences.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use Appendix B and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use Appendix B and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. Monitoring

The School reserves the right to monitor Network, Internet and Email activity, so that compliance with this policy and other relevant policies, regulations, and/or codes of practice that govern users' performance and/or conduct can be effectively managed.

Regular monitoring of **all** Network, Internet and Email activity, both business **and personal** will be undertaken, i.e. a continuous log will be maintained of websites visited and which user has visited them and a continuous log will be maintained which will record senders, recipients and the size of messages

The School may also **exceptionally** check the **content** of both business **and personal** email messages sent by users to:

- detect or investigate alleged improper use of the system as detailed above
- to provide evidence for disciplinary investigations, where email activity can be demonstrated to be relevant to the specific investigation
- detect or prevent crime (this is likely to be in collaboration with the Police)

Attempts to access restricted Internet sites will be regularly monitored by means of automatic 'hold' or 'stop' notice reports to the network manager.

This information may be used to:

- detect or investigate alleged improper use of the Internet
- to provide evidence for disciplinary investigations, where Internet activity can be demonstrated to be relevant to the specific investigation
- detect or prevent crime (this is likely to be in collaboration with the Police)

Such action will be proportionate to the suspected activity.

Usage infringements may be addressed by pre-warned or immediate suspension of user privileges, i.e. deactivation of the user's account. Such action may be taken by the responsible line manager and/or the network manager.

Requests for disciplinary purposes, involving either **business or personal** use, will be submitted to the Headmaster and the school's Data Protection Officer (DPO) in writing by the senior manager with responsibility for the user. Such requests must clearly state the purpose of the request in accordance with this policy.

The DSL logs behaviour and safeguarding issues related to online safety.

We have carefully considered and analysed the impact of this policy on equality and the possible implications for students with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Appendix A – Use of Email

1 Use of Email

1.1 The email facility is provided for official School use, although incidental and occasional personal use is permitted.

1.2 Email is not a secure method of transmission. It is possible, and likely, that messages may be intercepted and read by other than the intended recipient. Where personal and/or sensitive data is being transmitted via internal email it is recommended that this is sent via an attachment, which is password protected, e.g. a Word or Excel document. External e-mails containing personal and/or sensitive data must be encrypted.

1.3 Email communications should be handled in the same way as a letter, note or any other business communication. They may be contractually binding on the School.

1.4 Maintenance of email mailboxes is essential.

- During term time email boxes should be opened at least once daily (Monday to Friday)
- only messages that are pending a response and/or action should be retained in an email mailbox
- all email messages that are required for longer term use should be stored in folders, i.e. on the local hard drive or other folders outside of the mail system
- all other email messages, return receipts and attachments should be deleted at the beginning of each half term. The deleted items folder should also be cleared at these times.

Note: *deletion will not remove the item, merely the 'tag' which identifies the item. The email will be retained in some form of back-up media, in accordance with the approved retention period, and may be produced in Court if this became a requirement.*

1.5 There should be no comments made in an email that could be used against the School in litigation. For example, statements of untrue facts that damage the reputation of a person or company or hold him/her up to hatred, ridicule or contempt, are libellous. They need not be insulting.

1.6 Large email attachments should be compressed wherever possible.

1.7 Email should be used wherever possible to distribute notes of meetings or any other similar documentation that is generated on a regular basis and has a consistent set of recipients.

1.8 Email messages should only be printed out in exceptional circumstances, not as a matter of course.

1.9 The 'reply all' function should not be used unless everyone in the original message needs a response.

1.10 The 'reply with history' function should not be used unless absolutely necessary. Replies have a document link in the subject field that can be used to view previous emails.

1.11 Ensure that computers are locked whenever they are left unattended.

1.12 All emails sent in the course of working at Bournemouth School should be sent from a Bournemouth School email account. Personal data shared outside of the school system should be in line with the Data Protection Policy.

2. Mass Mailings

2.1 Mass mailings are both time consuming and expensive. A broadcast message should only be sent after alternative means of communication have been investigated.

3. Prohibited Email Activities

3.1 The following email activities may prompt disciplinary action up to, and including, dismissal:

- forging of email messages or attachments, i.e. forging your user ID by sending messages from another employee's computer without their knowledge or consent
- reading, deleting, copying or modifying the contents of another person's email mailbox without consent or other appropriate authority
- sending offensive, insulting, bullying, racist, obscene or threatening email (n*ote: the mass mailing of jokes is ill advised, some people may find the content of such jokes offensive)*
- sending chain letters
- transmission of files in direct violation of licensing and/or copyright laws
- the promotion of ventures, causes or organisations outside of Bournemouth School, or solicitations for personal profit
- sending or forwarding jokes with graphics attached. If received these must be immediately deleted and the sender informed that the receipt of such messages is not permitted. For persistent offenders incoming emails can be barred
- making comments in an email that could be used against the School in litigation

4. Personal Use of Email

4.1 **IMPORTANT NOTE**: Users who use the system for personal email messages expressly consent to the conditions detailed in this policy. If users do not accept the conditions under which the School's email system can be used for personal purposes then they must not use the system to send or receive personal messages.

4.2 Incidental and occasional personal use of email, within employees' own time, is permitted.

4.3 Such use is under the conditions detailed in this policy and users should note in particular the section relating to the monitoring of email.

4.4 The School does not provide separate, private email mailboxes for users and it is not, therefore, possible to differentiate between **personal** and **school** email messages. In view of this personal messages **cannot** be regarded as private and confidential.

5. Message Protocol

5.1 **Integrity of messages**

All messages will be deemed to be genuine, complete, accurate and secure against being altered in the course of transmission. Users must immediately notify any sender/recipient, their Line Manager and the network manager if there is any suspicion that this is not the case

5.2 **Authenticity of messages**

All messages must identify the sender and all recipients of that message.

5.3 **Security of messages**

- all users shall take reasonable care to ensure that all messages are securely stored, are not accessible to unauthorised persons, are not altered, lost or destroyed, and are capable of being retrieved only by properly authorised persons

- all users are responsible for ensuring that they have reasonable security systems and procedures to prevent the unauthorised access and sending of messages from their system

- all users shall use their respective best endeavours to ensure that no message contains a virus

Appendix B – Internet Use

1. Internet Use

1.2 The Internet facility is provided for official business use, although incidental and occasional personal use is permitted.

1.3 The School provides Internet access to assist users to perform their duties more efficiently and to enable them to be part of a well-informed educational community.

1.4 You are responsible for ensuring that you use the Internet facility in an effective, lawful and ethical manner with respect for the privacy and rights of other individuals.

1.5 There should be no Internet activity that could be used against the School in litigation, e.g. posting statements of untrue facts on websites that damage the reputation of a person or company or hold her/him up to hatred, ridicule or contempt, are libelous. They need not be insulting.

1.6 Internet usage for business purposes must be **focused** and **topic-specific**. Browsing the Internet in the hope of finding school related items of interest is likely to cause network and server congestion. It may slow down other users, reduce the amount of time available for productive work, and consume shared resources.

1.7 Information obtained from the Internet should be treated in the same way as any other information gathered from a public source. Do not assume that information is correct unless you know the source to be reputable and reliable.

1.8 You must have virus protection software installed on your PC to prevent possible virus infection from files downloaded from the Internet.

1.9 If you receive any system messages or system warnings that are unfamiliar you should contact the network manager for advice/assistance.

1.10 Ensure that your PC is locked whenever it is left unattended.

2. Prohibited Internet Activities

2.1 The following Internet activities may prompt disciplinary action up to, and including, dismissal:

2.1.1 forging Internet usage, i.e. forging your user ID by accessing the Internet via another employee's computer without their knowledge or consent

2.1.2 posting offensive, insulting, bullying, racist, obscene or threatening information on the Internet

2.1.3 accessing or attempting to access pornographic and other restricted sites, i.e. those categorised as 'adult content'

2.1.4 using the Internet to engage in Chat, Games or Talk services, which will be perceived as intentionally depriving other users of educational resources

2.1.5 using files downloaded from the Internet in direct violation of licensing and/or copyright laws

2.1.6 promoting ventures, causes or organisations outside of the School or using Internet resources to initiate negotiations with others for personal financial gain or solicit for personal profit

2.1.7 posting information on the Internet that could be used against the School in litigation

3. Personal Use of the Internet

3.1 **IMPORTANT NOTE:** Users who make personal use of the School's Internet facility expressly consent to the conditions detailed in this policy.

3.2 If users do not accept the conditions under which the School's Internet facility can be used for personal purposes **then they must not use the system for such purposes.**

3.3 Incidental and occasional use of the School's Internet service, within the user's own time, is permitted.

3.4 Such use is under the conditions detailed in this policy and users should note in particular the section relating to the monitoring of Internet usage.

3.5 The School does not provide separate, private access to the Internet and it is not, therefore, possible to differentiate between **personal** and **school** use. In view of this personal use of the Internet should not be regarded as private or confidential. Users **cannot have any expectation of privacy** when they access the Internet using the School's equipment and network facilities.

Appendix C – Students' Acceptable Use of ICT Code of Conduct

1. Students' Acceptable Use of ICT Code of Conduct

2. You must follow the following guidelines if you wish to have access to the School's ICT resources.

3. All users of the Network, Internet and email are expected to abide by these rules of computer and network use:

- Be polite when using email.
- Do not use email to bully or insult others
- Do not use inappropriate or unacceptable language
- Never reveal your personal address or telephone number or those of fellow students to people unknown to you
- Email is not private. We scan and periodically sample. Never say anything or engage in anything that you would not be happy to write on a postcard that could be read by everyone
- Inform a member of staff **IMMEDIATELY** should you discover an obscene or offensive web page so that its access can be blocked

4. Students agree that they will **not** perform the following unacceptable actions:

- Try to bypass the internet security
- Complete questionnaires or subscription forms without checking with a member of staff
- Damage, degrade or disrupt the performance of equipment or systems
- Attempt to retrieve information about 'hacking' or attempt to 'hack' our system
- Download programmes
- Play games that have not been placed on the network by the school administrators
- Send or display offending messages, pictures, videos or sound
- Take part in on-line newsgroups or chat lines
- Use the Internet to buy or sell anything
- Use the Internet to access obscene or offensive web pages/material
- Use the network for any illegal activity, including the violation of copyright or other laws
- Use the network in ways that break the school rules and standards of behaviour
- Use someone else's account, either with or without permission
- Tell another student their password

5. The school will electronically audit Internet and email usage at all times and a record of this is kept.

6. Abusing the school's network or internet will result in appropriate sanctions which may include:

- Loss of access to the Internet
- Loss of access to the school email
- Loss of access to the school network
- Disciplinary action (including exclusions)
- Involvement of external agencies, if necessary, including the police
- Paying for wastage/damage

Note
No student will be granted access to the Internet without both the student and parent/carer signing the Acceptable Use Agreement Appendix H. The agreement confirms that the student has read and agrees to abide by the Students' Acceptable Use of ICT Code of Conduct.

Appendix D – Staff, Governor, Volunteer and Visitors' Acceptable Use of ICT Code of Conduct

1. Acceptable Use of ICT Code of Conduct for Staff, Governor, Volunteer and Visitors'.

1.2 All adults using ICT equipment within the school must ensure that they have read and abide by the Use of ICT Policy and its appendices. If they are found to have contravened any of the requirements they may face disciplinary action.

1.3 Users are encouraged to make effective use of Internet and email. Such use should always be lawful and appropriate. It should neither compromise the school's computer systems nor have the potential to damage its reputation.

1.4 The school's ICT systems and network cannot be regarded as private, and user accounts will be subject to random monitoring. They should be used primarily for school purposes but **occasional** personal use is permitted. All ICT activities must conform to the norms of moral decency and not contravene ICT or other relevant legislation.

2. When using ICT equipment staff, governor, volunteer and visitors' will not

- give anyone access to their login name or password
- attempt to introduce any unlicensed applications
- corrupt, interfere with or destroy any other user's information
- release personal data relating to any colleague or student over the Internet
- use the school internet access for business, profit, advertising or political purposes
- enable access to personal data by leaving their account open at the end of a session
- engage in any activity which might compromise the security of the school network

3. When using e-mail staff, governors, volunteers and visitors will:

- adhere to the school's published guidelines. Email should not be considered a private medium of communication and great care should always be taken over content, because of the possibility of public scrutiny
- not include offensive or abusive language in messages nor any language which could be considered defamatory, obscene, menacing or illegal
- not use language that could be calculated to incite hatred against any ethnic, religious or other minority
- make sure that nothing in messages could be interpreted as libellous
- not send any message which is likely to cause annoyance, inconvenience or needless anxiety
- not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes
- as email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- only share personal data in accordance with the Data Protection Policy

4. When using the Internet staff, governor, volunteer and visitors' will:

- watch for accidental access to inappropriate materials and report any offending site so that action can be taken
- check copyright before publishing any work and ensure that any necessary permissions are obtained
- ensure that the school's photo policy is strictly adhered to

- report any breaches of the Internet policy

Note *No staff, governor, volunteer or visitor will be granted access to the Internet without signing the Acceptable Use Agreement Appendix I. The agreement confirms that the member as above has read and agrees to abide by the Staff, Governor, Volunteer and Visitor Acceptable Use of ICT Code of Conduct.*

Appendix E - Steps you can take to help prevent security problems

There are plenty of things that you should do (or not do) that will greatly reduce the risks of sensitive information going missing or being obtained illegally. Many of these 'dos and don'ts' will apply to how you handle your own personal information. Using these practices will help you to protect your own privacy.

1. Working online

Do:

- make sure that you follow the School's policies on keeping computers up to date with the latest security updates. Make sure that you keep any computers that you own up to date. Computers need regular updates to their operating systems, web browsers and security software (anti-virus and anti-spyware). Get advice from the network manager if you need help
- only visit websites that are allowed by the School's filtering system. Remember that the School may monitor and record (log) the websites you visit
- turn on relevant security warnings in your web browser (for example, the automatic phishing filter available in Internet Explorer and attack and forgery site warnings in Mozilla Firefox)
- make sure that you only install software that your network manager has checked and approved
- be wary of links to websites in emails, especially if the email is unsolicited
- only download files or programs from sources you trust. If in doubt, talk to the network manager

2. Email and messaging

Do:

- read and follow guidance contained within 'Appendix A' of this policy
- report any spam or phishing emails to the network manager that are not blocked or filtered
- report phishing emails to the organisation they are supposedly from
- use your School's contacts or address book. This helps to stop email being sent to the wrong address

Don't:

- click on links in unsolicited emails. Be especially wary of emails requesting or asking you to confirm any personal information, such as passwords, bank details and so on
- turn off any email security measures that the School has put in place or recommended
- email sensitive information unless you know it is encrypted
- try to bypass your organisation's security measures to access your email off-site (for example, forwarding email to a personal account)
- reply to chain emails

3. Passwords

Do:

- use a strong password (strong passwords are eight characters or more and contain upper and lower case letters as well as numbers)
- make your password easy to remember, but hard to guess
- choose a password that is quick to type
- use a mnemonic (such as a rhyme, acronym or phrase) to help you remember your password. Change your password(s) if you think someone may have found out what they are

Don't:

- share your passwords with anyone else
- write your passwords down
- use your work passwords for your own personal online accounts
- save passwords in web browsers if offered to do so
- use your username as a password
- use names as passwords
- email your password or share it in an instant message

4. Laptops

Do:

- shut down your laptop using the ‘Shut Down’ or ‘Turn Off’ option
- try to prevent people from watching you enter passwords or view sensitive information
- turn off and store your laptop securely (if travelling, use your hotel’s safe)
- use a physical laptop lock if available to prevent theft
- lock your desktop when leaving your laptop unattended
- make sure your laptop is protected with encryption software

Don’t:

- leave your laptop unattended unless you trust the physical security in place
- use public wireless hotspots – they are not secure
- leave your laptop in your car. If this is unavoidable, temporarily lock it out of sight in the boot
- let unauthorised people use your laptop
- use hibernate or standby

5. Sending and sharing

Do:

- be aware of who you are allowed to share information with. Check with the School’s Data Protection Officer (DPO) if you are not sure
- ask third parties how they will protect sensitive information once it has been passed to them
- encrypt all removable media (USB pen drives, CDs, portable drives) taken outside your organisation or sent by post or courier

Don’t:

- send sensitive information (even if encrypted) on removable media (USB pen drives, CDs, portable drives) if secure remote access is available
- send sensitive information by email unless it is encrypted
- place protective labels on outside envelopes. Use an inner envelope if necessary. This means that people can’t see from the outside that the envelope contains sensitive information
- assume that third-party organisations know how your information should be protected

6. Working on-site

Do:

- lock sensitive information away when left unattended
- use a lock for your laptop to help prevent opportunistic theft

Don’t:

- let strangers or unauthorised people into staff areas
- position screens where they can be read from outside the room

7. Working off-site

Do:

- only take offsite information you are authorised to and only when it is necessary. Ensure that it is protected offsite in the ways referred to above
- wherever possible access data remotely instead of taking it off-site
- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any services you have used
- try to reduce the risk of people looking at what you are working with
- leave your laptop behind if you travel abroad (some countries restrict or prohibit encryption technologies)

Appendix F - E-safety Rules

Ask permission before using the internet.

Tell a trusted adult if you see anything that make you feel uncomfortable.

Immediately close any webpage that you are uncomfortable with.

Do not give out any personal information such as name, address, telephone number(s), age, school name or bank card details.

Make sure that when using social networking sites, privacy settings are checked so that not just anyone can see your page/photos.

Only contact people that you have actually met in the real world.

Never arrange to meet someone that you have only met on the internet.

Only use a webcam with people you know.

Think very carefully about any pictures that you post online. Turn location services off when taking photos to avoid this information being imbedded into your photo and therefore available to anyone who sees the photo.

Never be mean or nasty to anyone on the internet. If you know of someone being mean to another person, tell a trusted adult.

Only open emails from people that you know.

Avoid using websites that you wouldn't tell anyone about and use a student friendly search engine such as http://www.askforkids.com

Report internet abuse using 'Think U Know'

Follow the school rules regarding mobile phones and electronic devices.

Appendix G – Use of Electronic Devices

For students in Years 7-11 we operate an 'on site out of sight' policy at all times which means the following:

- Students are not allowed to use a mobile phone or other electronic device (e.g. earpods) at any time between 08:00 and 15:30 in school. For emergency mobile phone use only (e.g. arranging for collection after school due to sports fixture cancellation), students must attend their pastoral office for express permission to use the office phone/their mobile phone.
- Smart watches are banned.
- If a student is caught using an electronic device in school, it will be confiscated and the following implemented:

Sanctions

1st occasion	Device will be returned to students at the end of the day and a warning given.
2nd occasion	After school detention
3rd and subsequent occasions	After school detention and the student will hand it in every day at reception for the remainder of the half term.

For sixth form students, mobile phones and electronic devices (e.g. earpods), can only be used in the following areas at the following times:

Sixth Form Study Centre	At all times
Le Bistro	At all times EXCEPT 10:15 – 10:35 and 12:20 – 13:45
Library Computer Room	At all times EXCEPT 10:15 – 10:35 and 12:20 – 13:45
In lessons	When directed to be a teacher for work related tasks only

Should a sixth form student be caught using a mobile phone or other electronic device (e.g. earpods), outside of the permitted areas and times, it will be confiscated and the same sanctions used for Years 7-11 implemented.

The above information may also be found in the school's Behaviour, Exclusions and Drugs Policy.

Appendix H - Acceptable Use Agreement (students and parent/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS, INTERNET AND MOBILE PHONE USE: AGREEMENT FOR STUDENTS AND PARENT/CARERS	
Name of student:	
I have read and will follow the rules in the E-Safety and Acceptable Use Policy and agree to the Students' Acceptable Use of ICT Code of Conduct **In Summary:** **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • In Years 7-11: I will comply with the requirement 'on site out of sight' between 08:00 and 15:30 • In sixth form: I can use it only in the Study Centre (all times), in lesson times when directed by a teacher, and in Le Bistro and library computer room with exception to 10:15 to 10:35 and 12:20 to 13:45 • When permitted, I will use it responsibly, and will not access any inappropriate websites or other inappropriate material, or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I do not follow the rules.**	
Signed (student):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix I: Acceptable Use Agreement (staff, governor, volunteer and visitors')

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNOR,VOLUNTEER AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
I have read and will follow the rules in the E-Safety and Acceptable Use Policy and agree to the Staff, Governor, Volunteer and Visitors' Acceptable Use of ICT Code of Conduct **In Summary:** **When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:** • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of students without checking with teachers first • Share confidential information about the school, its students or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Document Title	**Acceptable Use and E-Safety Policy**
Status	Statutory
Source	The Key
Review Period	Every 3 years
Last reviewed on:	November 2023
Next review due by:	November 2026

Document History

Version	Review Date	Author	Change/Notes
1.1	10/11/2020	J Wheatley	This document must be reviewed at the same time as the data protection policy to ensure consistency.
1.2	15/10/2021	C Lea	Document layout changed
1.2.1	09/02/2022	C Lea	Addition of the Public Sector Equality Duty (PSED) statement
1.3	06/11/2023	L Domeney	Annual Review: Section 1, updated to include '4 key categories of risk' Section 3, updated to reflect • governors roles and responsilbities to online safety (KCSiE 2023 guidance) • DSL responsibility to school filtering and monitoring Section 5, updated to reflect how we keep parents informed about online safety (KCSiE 2022 guidance) Section 6.3, Artificial Intelligence (AI) guidance added Section 7, Prevention, detections and investigation of misuse: Updated • in line with updated guidance from the DfE on searching, screening and confiscation • to clarify procedures if a staff member believes a device may contain a nude or

			semi-nude image, or an image that it's a criminal offence to possess Appendix G, RAG chart removed and mobile phone use added Appendix H: updated with • 'I will not create, link to or post..' • mobile phone access for all year groups updated

Approvals

Date of FGB Approval	**Approving Committee**
8/12/2020	Resources
21/11/2023	Resources
Nov 2026	