

|  |
| --- |
| BENTLEY NEW VILLAGE PRIMARY SCHOOL |
| Online Safety |
| Updated: Sept 2025 |

|  |
| --- |
| Headteacher: Victoria Simmons |

Contents

[1. Statement of intent 2](#_Toc162906988)

[2. Legal framework 2](#_Toc162906989)

[3. Roles and responsibilities 3](#_Toc162906990)

[3.1 The governing board 3](#_Toc162906991)

[3.2 The headteacher 3](#_Toc162906992)

[3.3 The designated safeguarding lead 3](#_Toc162906993)

[3.4 The ICT Support 4](#_Toc162906994)

[3.5 All staff and volunteers 4](#_Toc162906995)

[3.6 Parents 5](#_Toc162906996)

[3.7 Visitors and members of the community 5](#_Toc162906997)

[4. Educating pupils about online safety 5](#_Toc162906998)

[5. Educating parents about online safety 6](#_Toc162906999)

[6. Handling online safety concerns 6](#_Toc162907000)

[6.1 Cyber-bullying 6](#_Toc162907001)

[Definition 6](#_Toc162907002)

[Preventing and addressing cyber-bullying 7](#_Toc162907003)

[Examining electronic devices 7](#_Toc162907004)

[7. Acceptable use of the internet in school 7](#_Toc162907005)

[8. Pupils using mobile devices in school 8](#_Toc162907006)

[9. Staff using work devices outside school 8](#_Toc162907007)

[10. How the school will respond to issues of misuse 8](#_Toc162907008)

[11. Training 8](#_Toc162907009)

[12. Monitoring arrangements 8](#_Toc162907010)

[13. Links with other policies 8](#_Toc162907011)

[Appendix 1: Pupil Acceptable Use Agreement 10](#_Toc162907012)

[Parent or Guardian Permission 11](#_Toc162907013)

[Appendix 2: Workforce Acceptable Use Agreement 12](#_Toc162907014)

[Introduction and Scope 12](#_Toc162907015)

[Email and Internet Use 12](#_Toc162907016)

[Personal Use 12](#_Toc162907017)

[Inappropriate Use 12](#_Toc162907018)

[Other Business Use 12](#_Toc162907019)

[Security 13](#_Toc162907020)

[Group Email Accounts 13](#_Toc162907021)

[Social Media Use 13](#_Toc162907022)

[Corporate Accounts 13](#_Toc162907023)

[Personal Accounts 13](#_Toc162907024)

[Telephone and Video Conferencing Use 14](#_Toc162907025)

[Personal Use 14](#_Toc162907026)

[Inappropriate Use 14](#_Toc162907027)

[Other Business Use 14](#_Toc162907028)

[Personal Devices 14](#_Toc162907029)

[Permitted Activity 14](#_Toc162907030)

[Device Security 15](#_Toc162907031)

[Data Breaches 16](#_Toc162907032)

[Authorised Access 16](#_Toc162907033)

[Exemption Process 16](#_Toc162907034)

[Appendix 3: online safety training needs – self-audit for staff 17](#_Toc162907035)

[Appendix 4: Online safety and the curriculum 18](#_Toc162907036)

# 1. Statement of intent

Bentley New Village Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

• Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.

• Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.

• Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.

• Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk.

Our school aims to:

* Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
* Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
* Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

# 2. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

• Voyeurism (Offences) Act 2019

• The UK General Data Protection Regulation (UK GDPR)

• Data Protection Act 2018

• DfE (2021) ‘Harmful online challenges and online hoaxes’

• DfE (2023) ‘Keeping children safe in education 2022’

• DfE (2019) ‘Teaching online safety in school’

• DfE (2018) ‘Searching, screening and confiscation’

• Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’

• UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’

• National Cyber Security Centre (2018) ‘Small Business Guide: Cyber Security’

# 

# 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 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 governor who oversees online safety is Ruth Precious

All governors will:

* Ensure that they have read and understand this policy
* Agree and adhere to the terms on acceptable use of the school’s ICT systems and the internet (appendix 2)
* Reviewing this policy on an annual basis.
* Ensuring their own knowledge of online safety issues is up-to-date.
* Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
* Ensuring that there are appropriate filtering and monitoring systems in place.
* Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

### 3.2 The headteacher

Ensuring that online safety is a running and interrelated theme throughout the school’s policies and procedures, including in those related to the curriculum, teacher training and safeguarding.

* Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
* Ensuring online safety practices are audited and evaluated.
* Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
* Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
* Working with the DSL and ICT technicians to conduct termly light-touch reviews of this policy.
* Working with the DSL and governing board to update this policy on an annual basis.

### 3.3 The designated safeguarding lead

Details of the school’s designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

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
* Acting as the named point of contact within the school on all online safeguarding issues
* Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
* Ensuring online safety is recognised as part of the school’s safeguarding responsibilities and that a coordinated approach is implemented
* Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
* Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
* Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)
* 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.
* Keeping up-to-date with current research, legislation and online trends.
* Supporting the ICT lead in the school’s participation in local and national online safety events, e.g. Safer Internet Day.

### 3.4 The ICT Support

The ICT Support Officer is responsible for:

* Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils 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 monthly 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 (see appendix 4) 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 2), and ensuring that pupils follow the school’s terms on acceptable use (appendix 1)

* Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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
* Taking responsibility for the security of ICT systems and electronic data they use or have access to.
* Modelling good online behaviours.
* Maintaining a professional level of conduct in their personal use of technology.
* Having an awareness of online safety issues.
* Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
* Reporting concerns in line with the school’s reporting procedure.
* Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

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 of the school’s ICT systems and internet (appendix 1)

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

* What are the issues?, UK Safer Internet Centre: [https://www.saferinternet.org.uk/advicecentre/parents-and-carers/what-are-issues](https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues)
* Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
* Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

### 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 2).

3.8 Pupils

Pupils are responsible for:

• Adhering to the Acceptable Use Agreement and other relevant policies.

• Seeking help from school staff if they are concerned about something they or a peer have experienced online.

• Reporting online safety incidents and concerns in line with the procedures within this policy.

# 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

* Use technology safely and respectfully, keeping personal information private
* Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies Pupils in **Key Stage 2** will be taught to:
* Use technology safely, respectfully and responsibly
* Recognise acceptable and unacceptable behaviour
* Identify a range of ways to report concerns about content and contact

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 pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils 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.

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. Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

* Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened.
* Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.
* Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future.
* Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim’s wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim’s parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress. Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children’s social care or the police against the victim’s wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member’s online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures.

If the concern is about the Headteacher, it is reported to the Chair of Governors.

Concerns regarding a pupil’s online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Headteacher and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher contacts the police. The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy. All online safety incidents and the school’s response are recorded by the DSL.

## 

## 6.1 Cyber-bullying

### 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.)

### Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils 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 pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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 pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets 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 pupils, 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.

### Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils’ electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a ‘good reason’ to do so.

When deciding whether there is a good reason to examine or erase 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, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

* Delete that material, or
* Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
* Report it to the police

Any searching of pupils will be carried out in line with the DfE’s latest guidance on [screening, searching and confiscation.](https://www.gov.uk/government/publications/searching-screening-and-confiscation)

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

# 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school’s ICT systems and the internet (appendices 1 and 2). 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 pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

# 8. Pupils using mobile devices in school

Pupils may bring mobile devices into school in special circumstances, however they are to be left with the office staff for safe keeping until they are needed/the end of the day.

# 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 2.

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. How the school will respond to issues of misuse

Where a pupil misuses the school’s ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school’s ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

# 11. Training

All new staff members will receive training, as part of their induction, on safe internet use 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 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 arrangements

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

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

# 13. Links with other policies

This online safety policy is linked to our:

* Child protection and safeguarding policy
* Managing Emotions and Behaviour policy
* Staff disciplinary procedures
* Data protection policy and privacy notices
* Complaints procedure
* Social Media Policy
* Whistleblowing Policy
* Acceptable Use Agreement
* Anti-Bullying Policy
* PSHE Policy
* RSE and Health Education Policy
* Staff Code of Conduct
* Confidentiality Policy

# Appendix 1: Pupil Acceptable Use Agreement

**Introduction**

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should be entitled to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

* our pupils will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use,
* school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk, and
* parents and guardians are aware of the importance of e-safety and are involved in the education and guidance of young people regarding on-line behaviour.

Pupil Acceptable Use Agreement

* I understand that while I am a member of Bentley New Village Primary School I must use technology in a responsible way.
* I will ask a teacher or suitable adult if I want to use the computers.
* I will only use activities that a teacher or suitable adult has told or allowed me to use.
* I will take care of the computer and other equipment.
* I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
* I will tell a teacher or suitable adult if I see something that upsets me on the screen.
* I know that if I break the rules I might not be allowed to use a computer.

I have read and understand the above and agree to follow these rules when:

* I use the school systems and devices (both in and out of school).
* I use my own equipment outside of school in a way that is related to me being a pupil of Bentley New Village Primary School e.g. communicating with other pupils or teachers, accessing school email, website etc.

**Pupil name: Class:**

**Pupil signature: Date:**

## 

## Parent or Guardian Permission

* As the parent of guardian of the above pupil, I give permission for my child to have access to the internet and to ICT systems at school.
* I know that my child has signed this Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
* I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.
* I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
* I understand that my child’s activity on ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
* I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child’s e-safety.

**Parent or guardian name:**

**Parent or guardian signature:**

**Date:**

# Appendix 2: Workforce Acceptable Use Agreement

### Introduction and Scope

The Acceptable Use policy includes accessing cloud services on personal devices and governs the use of Bentley New Village’s corporate network and cloud-based systems that individuals use on a daily basis in order to carry out business functions.

This policy applies to all employees, governors or trustees, contractors, agents and representatives, volunteers and temporary staff working for, or on behalf of, the school.

This policy should be read in conjunction with the other policies in our information governance policy framework, including the Data Protection policy, Information Security policy and Records Management policy.

### Email and Internet Use

We provide email accounts and internet access to the workforce to assist with performance of their duties. We also allow the workforce to use its instant messaging service. For the benefit of doubt Instant Messages are classed as email communications in this policy.

### Personal Use

Whilst email accounts and the internet should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as:

* Personal messages or internet usage do not tarnish our reputation, or infringe on business functions,
* Users understand that emails sent to and from corporate accounts are the property of the Bentley New Village,
* Users understand that we may have access to their email account and any personal messages contained within,
* Users understand that we may have access to their internet browsers and browsing history contained within,
* Users understand that emails sent to or from their email account may have to be disclosed under Freedom of Information and/or Data Protection legislation,
* Users understand that we reserve the right to cleanse email accounts at regular intervals which could result in personal emails being erased from the corporate network,
* Users understand that we reserve the right to suspend internet access at any time.

### Inappropriate Use

We do not permit individuals to send, forward, or solicit emails, or use the internet in any way that may be interpreted as insulting, disruptive, or offensive by any other individual or entity. Examples of prohibited material include, but are not necessarily limited to:

* Sexually explicit or pornographic messages, images, cartoons, jokes or movie files,
* Unwelcome propositions, profanity, obscenity, slander, or libel,
* Any messages or content containing ethnic, religious, political, or racial slurs,
* Any messages or content that could be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs.
* Users are also not permitted to use the internet in a way which could affect usage for others. This means not streaming or downloading media files and not using the internet for playing online games.

### Other Business Use

Users are not permitted to use emails or the internet to carry out their own business or business of others. This includes, but is not necessarily limited to, work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case-by-case basis at the discretion of Bentley New Village management.

### Security

Users will take care to use their email accounts and the internet in accordance with our Information Security policy. In particular users will:

* Not click on links from un-trusted or unverified sources,
* Use secure email transmission methods when sending personal data,
* Not sign up to marketing material that could jeopardise our IT network,
* Not send excessively large email attachments without authorisation from management and our IT provider.

### Group Email Accounts

Users may also be permitted access to send and receive emails from group and/or generic email accounts. These group email accounts must not be used in a personal capacity and users must ensure that they sign each email with their name so that emails can be traced to individuals. Improper use of group email accounts could lead to suspension of a user’s email rights.

Headteacher will have overall responsibility for allowing access to group email accounts but this responsibility may be devolved to other individuals.

We may monitor and review all email traffic that comes to and from individual and group email accounts.

### Social Media Use

We recognise and embrace the benefits and opportunities that social media can contribute to an organisation. We also recognise that the use of social media is a data protection risk due to its open nature and capacity to broadcast to a large amount of people in a short amount of time.

### Corporate Accounts

We have a number of social media accounts across multiple platforms. Nominated users will have access to these accounts and are permitted to post general information about the Bentley New Village. Authorised users will be given the usernames and passwords to these accounts which must not be disclosed to any other individual within or external to the organisation. Headteacher will have overall responsibility for allowing access to social media accounts.

Corporate social media accounts must not be used for the dissemination of personal data either in an open forum or by direct message. This would be a contravention of our information governance policies and data protection legislation.

Corporate accounts must not be used in a way which could:

* Tarnish our reputation,
* Be construed as harassment or disparagement of others based on their sex, gender, racial or ethnic origin, sexual orientation, age, disability, religious or philosophical beliefs, or political beliefs,
* Be construed as sexually explicit,
* Be construed as political beliefs or commentary.

### Personal Accounts

We understand that many users will use or have access to personal social media accounts. Users must not use these accounts:

* During working hours,
* Using corporate equipment,
* To conduct corporate business,
* To contact or approach our clients, customers, or partners.

### Telephone and Video Conferencing Use

We provide users with access to telephone and video conferencing services to assist with performance of their duties.

### Personal Use

Whilst telephone and video conferencing services should primarily be used for business functions, incidental and occasional use in a personal capacity may be permitted so long as:

* Usage does not tarnish our reputation or infringe on business functions,
* Users understand that we may have access to call history and recordings,
* Users understand that we reserve the right to suspend telephone and video conferencing usage at any time,
* Telephone call or video conference recordings or transcripts may have to be disclosed under Freedom of Information and/or Data Protection legislation.

### Inappropriate Use

We do not permit users to use the telephone or video conferencing services in any way which may be interpreted as insulting, disruptive, or offensive by any other individual or entity.

### Other Business Use

Users are not permitted to use these services to carry out their own business or business of others. This includes work for political organisations, not-for-profit organisations, and private enterprises. This restriction may be lifted on a case-by-case basis at the discretion of Bentley New Village management.

### Personal Devices

We identify a personal device as any electronic device that has not been provided by us and can be used to access and process personal data, including data accessed from the cloud through an internet connection. This includes, but it not limited to:

* Laptop or PC
* Notebook
* iPad or tablet
* Smartphone

Use of the device must be limited to the individual user, and not be shared resources (e.g. a family device).

### Permitted Activity

Whilst using their own devices, users are permitted to access, review and process personal data within the school system in which it is held. Users must only access data they are entitled to in order to fulfil their duties.

It is not permitted for any school data to be downloaded and saved onto any personal device under any circumstances. All school data must remain within the defined systems to ensure it remains secure, available to all authorised personnel and held within our records management system for its full lifecycle, including secure destruction in line with our retention schedule.

By retaining data within school-controlled systems, in the event of an individual exercising their rights as detailed in the UK GDPR; particularly with the right to access (Subject Access Request), the searching criteria to meet a request will not require users to search their own devices for evidence of personal data that may have been stored.

Printing of any personal data to home printers is strictly forbidden. The storage and confidential disposal of paper documents cannot be easily managed and guaranteed when taken off the school site.

### Device Security

**Anti-virus and software security patching**

The range of devices currently available all present different levels of ability to apply appropriate security and protection to the equipment. It is therefore the responsibility of the user to ensure that all available protection and security is applied. Specialist advice should be sought where appropriate.

We require that any device used for accessing school systems in the cloud must have adequate anti-virus software. The software should be installed, configured and maintained by a suitably qualified or experienced person. All available updates must be applied in a timely manner.

Out of date software (including operating systems) can provide vulnerabilities that can be exploited by unscrupulous hackers. All software installed on devices that is going to be used to access school data must be operating at the most up to date version with all security releases applied. All software should be configured and maintained by a suitably qualified or experienced person for the full period that they are used to access school data.

**Password/PIN protection**

All devices must be secured by a unique password or security pin to ensure that access to the device is limited to the named user permitted to access the school’s personal data. Devices that lack the ability to enforce this level of security must not be used to access school data.

Data on personal devices is unlikely to be encrypted, and therefore particularly vulnerable if lost or stolen. Having a robust password or PIN in place provides an additional layer of protection.

**Personal applications (apps)**

Users are asked to be mindful of the apps installed on personal devices that are used to access school data. Some of these apps may have enhanced privileges and tracking within them that monitor use of the device and other items that are being accessed. This should be detailed in the application’s terms and conditions and the user should seek assurance that this risk is being effectively managed.

**Equipment disposal**

When a device being used to access school information is disposed of, it is the responsibility of the user to ensure that no records or school data have found their way onto the device, either accidently or for a temporary purpose, prior to surrendering it as a part of an upgrade process, at point of resell or for permanent disposal through the WEEE (Waste Electronic and Electrical) process. Specialist advice should be sought where appropriate.

**Physical security**

Users should ensure any device used to access school data is kept safe and secured to prevent theft or damage. This includes actions such as not leaving devices overnight in cars, unattended in public spaces, or transported without sufficient protection to prevent accidental damage.

**System and Accounts Security**

When accessing data held in the cloud via an internet connection (e.g. Microsoft 365), users must ensure that their account is closed when not in use by logging out of the system. It is not permitted for accounts to be left open when not in use, if accessing school systems.

Users are responsible for ensuring any internet connection used to access school data is secured through the use of access controls, such as using a designated username and password. Unsecured network connections (Wi-Fi or hot spots) must not be used, and devices must be configured to prevent automatic connection to unknown networks (e.g. cafes, shopping centres, library etc.).

### Data Breaches

In the event of a data breach users must follow the process detailed in the Information Security policy and report any suspected breach immediately.

Users are asked to be mindful of the following situations in which the risk of a data breach increases:

* Systems are not shut down appropriately when not in use, leading to unauthorised access of school data.
* Personal devices are shared with family, friends, or partners leading to unauthorised access of school data.
* Documents and files are downloaded onto shared devices, and then become accessible to other users of the device.
* Passwords or security PINs are shared with others (e.g. family and partners) leading to unauthorised access of school data.
* Inadequate management of security and software updates leaves a vulnerability to a virus or hack. Once unauthorised control of a device is established it is difficult to identify and remove.
* Disposal of devices that have not been adequately assessed and the permanent removal of any school related data prior to surrender.

### Authorised Access

Access to school systems using personal devices is only permitted whilst the user has authorisation to do so. In the event that the user leaves the employment of the school; or the relationship terminates for third parties and contractors; access should not be attempted. To do so would be treated as a data breach and investigated as such.

It is a criminal offence under Section 170 of the Data Protection Act 2018 to knowingly access data that you are not entitled to or after you have left our employment.

### Exemption Process

An exemption to any element of this policy can only be authorised by the school’s Senior Information Risk Owner (SIRO). Authorisation will only be given where there is a clear business need and following a full risk assessment to ensure risks are mitigated.

# 

# Appendix 3: online safety training needs – self-audit for staff

|  |  |
| --- | --- |
| **Online safety training needs audit** |  |
| **Name of staff member/volunteer:** | **Date:** |
| Do you know the name of the person who has lead responsibility for online safety in school? |  |
| Do you know what you must do if a pupil approaches you with a concern or issue? |  |
| Are you familiar with the school’s acceptable use agreement for staff, volunteers, governors and visitors? |  |
| Are you familiar with the school’s acceptable use agreement for pupils and parents? |  |
| Do you regularly change your password for accessing the school’s ICT systems? |  |
| Are you familiar with the school’s approach to tackling cyber-bullying? |  |

# Appendix 4: Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

• RSE

• Health education

• PSHE

• Citizenship

• ICT

Online safety teaching is always appropriate to pupils’ ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

• How to evaluate what they see online

• How to recognise techniques used for persuasion

• What healthy and respectful relationships, including friendships, look like

• Body confidence and self-esteem

• Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts

• Acceptable and unacceptable online behaviour

• How to identify online risks

• How and when to seek support

• How to identify when something is deliberately deceitful or harmful

• How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum. The DSL is involved with the development of the school’s online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the SENCO, work to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked: • Where does this organisation get their information from?

• What is their evidence base?

• Have they been externally quality assured?

• What is their background?

• Are they age-appropriate for pupils?

• Are they appropriate for pupils’ developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate. Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy. If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.