

Document Control	
Document Title:	Digital (incl Online) Safety
Date of Last Review:	September 2025
Next Review Due:	September 2026
Person Responsible:	Assistant Headteacher Pastoral

Digital (incl Online) Safety

Contents:

	Pages
Scope of the Policy	1
Roles and Responsibilities	1 - 4
Mobile Devices	4
Education – pupils	7
Education – parents / carers	7
Education & Training – Staff / Volunteers	8
Training – Governors	8
Technical – infrastructure / equipment, filtering and monitoring	8
Use of digital and video images	9
Data Protection	10
Communications	11
Social Media - Protecting Professional Identity	12
Responding to incidents of misuse	14
Appendices – Acceptable Use Agreements	17 - 25

Scope of the Policy

This policy applies to all members of the Banstead Preparatory School community, including staff, pupils, volunteers, parents/carers, visitors, and external users, who have access to and make use of the school's ICT systems, whether on the school premises or remotely.

It covers the use of all digital technologies, including (but not limited to):

- Computers, laptops, and tablets
- Mobile phones and smartwatches
- Internet-connected devices
- Email and messaging platforms
- Cloud-based services
- Social media and online collaboration tools

This policy is intended to ensure safe, responsible, and appropriate use of technology in all contexts relating to the school.

Legal and Behavioural Framework

The Education and Inspections Act 2006 gives Headteachers the authority to regulate pupil behaviour, including conduct off-site, where it relates to the school. This includes incidents involving cyberbullying, online harassment, or any other online safety concern that is connected to a child's membership of the school.

The Education Act 2011 extended these powers, allowing school staff to search for and, where necessary, delete data from electronic devices where there is reason to believe a breach of the school's behaviour or safeguarding policies has occurred (see appendix for further detail).

Any action taken under these provisions will be in accordance with the school's Behaviour Policy, Safeguarding and Child Protection Policy, and Anti-Bullying Policy.

Out-of-School Incidents

Banstead Preparatory School recognises that harmful or inappropriate online activity can occur outside school hours and off school premises. Where such incidents affect pupils or staff and are brought to the school's attention, they will be addressed in line with this policy.

Where appropriate, the school will:

- Investigate and respond to concerns
- Engage with parents/carers
- Provide support to pupils or staff involved
- Take action in line with disciplinary and safeguarding policies

Roles and Responsibilities

This section outlines the online safety roles and responsibilities of all individuals and groups within the Banstead Preparatory School community.

Governors

The Governing Body is responsible for:

- Approving and reviewing the school's Digital and Online Safety Policy.
- Ensuring that online safety is embedded within the school's safeguarding framework.
- Receiving regular updates regarding online safety incidents and trends.

A designated Online Safety Governor will:

- Meet regularly with the Online Safety Coordinator.
- Monitor the online safety incident log and filtering/change control logs.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No. 1016538) and ULT (Registered in England No. 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

- Report relevant findings to the governing board and appropriate committees.

Headteacher and Senior Leadership Team (SLT)

The Headteacher has overall responsibility for safeguarding, including online safety, and ensures that:

- The day-to-day management of online safety is delegated to a competent Online Safety Coordinator.
- All members of the SLT understand procedures in the event of a serious online safety incident, particularly those involving staff.
- Relevant staff receive appropriate and up-to-date training.
- There is a clear system for supporting those responsible for monitoring and managing online safety within the school.
- Regular reports on online safety are received from the Online Safety Coordinator.

Digital Lead

The Digital Lead is responsible for:

- Leading the online safety committee.
- Managing and reviewing the school's digital and online safety practices and policies.
- Ensuring staff understand procedures for reporting online safety incidents.
- Providing training and support to staff.
- Liaising with technical staff on digital security and filtering systems.
- Maintaining logs of incidents and ensuring they are used to inform future planning

Network Manager:

The network manager is responsible for ensuring:

- The school's IT infrastructure is secure, up to date, and protected against misuse or cyber threats.
- Compliance with technical requirements for filtering and monitoring, including those set by the Local Authority or trust (e.g., United Learning).
- Enforced password policies and user access control measures are in place.
- Filtering systems are regularly reviewed and updated, with responsibility shared among staff.
- Monitoring systems are implemented and managed to detect misuse.
- Misuse is logged and reported to the Headteacher or Online Safety Coordinator for investigation.

Teaching and Support Staff

All teaching and support staff must:

- Have an up-to-date understanding of online safety and follow the school's policy and practices.
- Sign and adhere to the Staff Acceptable Use Policy (AUP).
- Report any concerns or suspected misuse to the Headteacher or Online Safety Coordinator.
- Maintain professional digital communication with pupils and parents via official school systems only.
- Embed online safety into the curriculum and all digital learning activities.
- Support pupils in developing safe online behaviour, critical thinking, and an understanding of digital rights and responsibilities (e.g., copyright, plagiarism).
- Monitor pupils' use of digital devices during lessons and school activities, and address inappropriate use.
- Use pre-vetted websites for internet-based activities and know how to respond to accidental exposure to unsuitable material.

Child Protection/Safeguarding – DSL

The DSL is responsible for:

- Being trained in online safety, including recognising and responding to the safeguarding implications of:
 - Sharing personal data
 - Accessing inappropriate or illegal content
 - Online grooming or inappropriate adult contact
 - Cyberbullying or harassment
- Receiving and logging reports of online safety incidents.
- Liaising with the Local Authority or United Learning as needed.
- Meeting with the Online Safety Governor to review incident data and technical monitoring logs.
- Reporting regularly to the Senior Leadership Team and governing body.

Pupils:

Pupils are expected to:

- Use school digital systems responsibly and in accordance with the Pupil Acceptable Use Policy.
- Understand the importance of reporting unsafe, inappropriate, or upsetting online behaviour or content.
- Know the school's expectations for the use of mobile devices, cameras, and other digital technologies.
- Show respect for copyright and avoid plagiarism.
- Understand the impact of cyberbullying and their role in creating a safe online environment.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No: 1016538) and ULT (Registered in England No: 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

- Recognise that online safety rules apply both in and outside of school, especially when behaviour affects the school community.

Parents / Carers

Parents and carers play a key role in supporting their child's digital safety. They are encouraged to:

- Attend school-provided online safety workshops and engage with communications about digital wellbeing.
- Promote positive online behaviours and monitor their child's use of technology at home.
- Support the school's approach to digital safety, including use of school devices and guidance on sharing images or video taken at school events.
- Follow guidance for appropriate use of school-issued 1:1 devices (Years 3–6).
- Encourage their children to talk about their online experiences and report any concerns.

Mobile Devices Policy

Introduction

Banstead Preparatory School recognises the widespread use of mobile phones and other internet-enabled devices for communication, safety, and convenience. For practical and safeguarding reasons, staff may carry mobile phones and other personal devices; however, their use must be appropriate and should not interfere with the learning environment or the smooth running of the school.

To maintain a safe and focused educational setting, this policy outlines the expectations and restrictions regarding the use of mobile and connected devices by both staff and pupils.

Scope

This policy applies to all mobile and internet-connected devices, including but not limited to:

- Mobile phones (standard and smart)
- Tablets (e.g., iPads, Android devices)
- Laptops and netbooks
- Smartwatches and wearable devices
- Any other 3G/4G/5G or Wi-Fi-enabled technology

Staff Use of Mobile Devices

- Staff may bring personal mobile phones and devices to school for professional and personal use.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No. 1016538) and ULT (Registered in England No. 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

- Personal devices must be switched to silent or do not disturb mode during lessons, meetings, and when supervising pupils.
- Staff must not use personal devices for calls, messaging, or internet use in the presence of pupils unless in exceptional circumstances (e.g., emergency).
- Any photographs or videos of pupils must only be taken using school-owned devices, in accordance with safeguarding and data protection policies.
- Accessing or sharing inappropriate content via personal devices while on school premises or during school hours is strictly prohibited.
- Staff must store personal devices securely and out of sight when not in use.

Pupil Use of Mobile Devices

- Pupils are not permitted to use or carry personal mobile phones or connected devices during the school day.
- If a pupil needs to bring a phone to school for safety when travelling to or from school, it must be:
 - Clearly labelled with the pupil's name
 - Handed in to the school office upon arrival
 - Collected at the end of the school day
- Mobile devices brought to school without permission or not handed in will be confiscated and returned following a discussion with parents/carers.
- Pupils are expected to follow the school's Acceptable Use Policy regarding the use of digital devices, including those issued by the school in Years 3–6.

General Expectations and Safeguarding Considerations

- The use of any mobile device to bully, harass, record, or distribute inappropriate content is a serious breach of school policy and will result in disciplinary action in line with the Behaviour and Safeguarding Policies.
- The school reserves the right to inspect any personal device on the premises if there is reason to believe it has been used inappropriately or in violation of school policy (in line with the Education Act 2011).
- Devices with internet access must not bypass the school's internet filtering systems if used on school premises.

Visitors and Volunteers

- Visitors and volunteers must not use mobile phones in areas where pupils are present, except in designated staff or visitor areas.
- Any photographing or filming of pupils by visitors is not permitted without prior consent from the Headteacher.

Procedures

A Common-Sense Approach

Banstead Preparatory School adopts a common-sense, context-based approach to the use of mobile and Wi-Fi-enabled devices. While policies exist to maintain a safe and distraction-free environment, staff are trusted professionals and may exercise discretion in allowing mobile device use where educationally appropriate.

Permitted Use: Times and Locations

- Under teacher direction, pupils may use school-owned devices (e.g., iPads, digital cameras) to support learning by capturing photos, video, or audio to document their work.
- Use of personal mobile devices by pupils is not permitted during the school day; however, they may bring them for safety purposes when travelling to and from school, provided they are handed in at the school office.
- No content recorded on personal devices may be uploaded to social media, video-sharing platforms (e.g., YouTube), or image-sharing sites (e.g., Flickr) without the explicit permission of all individuals involved, including staff. Breaches may result in disciplinary action.

Restricted Use: Times and Locations

- Mobile devices must be switched off, muted, or in airplane mode during lessons, assemblies, and school activities, unless authorised by a teacher for learning purposes.
- Parental consent must be obtained for the school to record images or videos of pupils for internal use, even when using school devices.
- Staff should refrain from personal use of devices in the presence of pupils, unless in an emergency or professionally justified context.

Sanctions for Misuse of Mobile Devices

The misuse of mobile phones or other electronic devices will be addressed in line with the school's Behaviour Policy, Staff Code of Conduct, and other relevant policies. Sanctions may include:

- Confiscation of the device
- Parental contact or meeting
- Suspension of device privileges
- Formal disciplinary action (for serious or repeated offences)

Specifically:

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No. 1016538) and ULT (Registered in England No. 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

- Use of devices for bullying, harassment, intimidation, or sharing inappropriate images/texts is taken extremely seriously and will result in disciplinary action, which may include suspension or exclusion for pupils, or formal disciplinary procedures for staff.

Security of Personal Devices

- Staff and students are encouraged to security-mark their personal devices where possible.
- The school does not accept liability for loss, damage, or theft of personal electronic devices.
- Staff are advised to store devices securely, either on their person or in the staffroom. However, the school cannot guarantee the security of personal items left unattended.
- Staff should be aware that personal devices are not covered by the school's insurance policy.

Cyberbullying

All incidents of cyberbullying, whether occurring inside or outside of school, will be dealt with in accordance with the school's Care and Consideration (Anti-Bullying) Policy. This may lead to serious sanctions, including:

- Suspension, exclusion, or expulsion of pupils
- Formal disciplinary procedures in the case of staff (refer to the Staff Bullying and Harassment Policy)

Responding to Inappropriate Content on Mobile Devices

If a teacher suspects that a pupil has accessed or is storing inappropriate content on a personal device:

1. The device should be confiscated immediately and securely stored.
2. The matter should be referred to the Designated Safeguarding Lead (DSL) or a member of the Senior Leadership Team (SLT) for investigation.
3. Investigations will be carried out in line with the school's search and confiscation procedures, ensuring:
 - a. A second member of staff is present during any interview.
 - b. Parents/carers are informed and may be invited to attend the interview.
 - c. The Headteacher is informed of all developments.

Where the content is found to be seriously inappropriate or unlawful:

- The pupil may be suspended during the investigation, in line with the school's Exclusion, Expulsion, Removal and Review Policy.
- External agencies (such as the Local Authority or police) may be contacted as required.

Staff Mobile Devices and Safeguarding

If inappropriate images or content involving children or young people are discovered on a staff-owned mobile device, this must be:

- Reported immediately to the Headteacher, or in their absence, to a Designated Safeguarding Lead.
- Treated as a potential safeguarding concern, with actions taken in accordance with the school's safeguarding and whistleblowing procedures

Use of mobile devices: guidelines for staff use (photographs and videos)

EYFS and Whole School Policy

In accordance with the Statutory Framework for the Early Years Foundation Stage (EYFS), staff working in the EYFS setting at Banstead Preparatory School are strictly prohibited from using personal devices (e.g. mobile phones, personal cameras, tablets, smartwatches) to take photographs or videos of children for any reason.

This restriction has been extended to apply throughout the entire school to ensure consistency and to safeguard all pupils.

Only school-owned devices may be used to capture images or video of pupils for educational or professional purposes.

Policy Statements

1. Online Safety Education for Pupils

While filtering systems and technical safeguards are important, the most effective way to promote safe and responsible digital behaviour is through education. Banstead Preparatory School is committed to helping pupils recognise online risks, make informed choices, and build digital resilience.

Online safety education is delivered as follows:

- A planned online safety curriculum is integrated into Computing, PSHCEE, and other relevant lessons. It is revisited regularly and adapted as needed to remain relevant.
- Key messages about safe and responsible use of technology are reinforced through assemblies, pastoral sessions, and class discussions.
- Pupils are taught to:
 - Critically evaluate online content and verify information before accepting it as true.
 - Understand copyright and intellectual property rights, and acknowledge sources appropriately.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No. 1016538) and ULT (Registered in England No. 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

- Report any inappropriate or concerning content they encounter online.
- The Pupil Acceptable Use Agreement is explained clearly, and pupils are supported in understanding its importance both in and out of school.
- All staff model positive, responsible use of technology in their professional practice.
- Where internet access is planned, teachers guide pupils to age-appropriate, vetted websites and remain vigilant when supervising independent internet use.
- Where necessary for curriculum purposes (e.g., when researching sensitive topics such as drugs, racism, or discrimination), staff may request temporary access to blocked sites through the technical support team. All such requests must:
 - Be based on clear educational reasoning.
 - Be auditable and time-limited.

2. Online Safety Education for Parents and Carers

Parents and carers are key partners in promoting safe digital behaviour. However, many may be unaware of the frequency with which children encounter inappropriate or potentially harmful content online.

Banstead Preparatory School supports parents/carers by providing access to reliable guidance and information on online safety issues.

Awareness is raised through:

- Information shared during curriculum evenings, parent sessions, and workshops.
- Regular communications via letters, newsletters, the school website, and the Parent Portal.
- High-profile campaigns, such as Safer Internet Day and other national initiatives.
- Signposting to trusted resources (e.g. ThinkUKnow, Childnet, UK Safer Internet Centre) to help parents support their children at home.

3. Online Safety Education & Training for Staff and Volunteers

All staff and volunteers must understand their safeguarding responsibilities in relation to online safety. It is essential that they feel confident in recognising, responding to, and educating pupils about online risks.

Training and support will be provided as follows:

- A planned programme of formal training is made available to all staff, with updates provided regularly based on changing technology, risks, and national guidance.
- An audit of staff training needs is conducted periodically to ensure all staff are appropriately equipped.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No. 1016538) and ULT (Registered in England No. 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

- All new staff receive online safety training during their induction, including an introduction to the school's Online Safety Policy and Acceptable Use Agreements.
- The Digital Lead attends external training and reviews new guidance, ensuring the school's approach remains current.
- Policy updates are shared and discussed during staff meetings, INSET days, and briefings.
- The Online Safety Coordinator is available to provide ongoing advice, training, and individual support as needed.

4. Online Safety Training for Governors

Governors have a strategic role in safeguarding and must understand the implications of online safety. This is especially important for governors with responsibilities in safeguarding, health and safety, or technology.

Governors may receive training through:

- Local Authority, National Governance Association (NGA), or other external provider-led training sessions.
- Participation in school-led training or parent/carer information sessions.
- Attendance at assemblies or curriculum lessons to gain insight into how online safety is taught and modelled across the school.

Technical – infrastructure / equipment, filtering and monitoring

Banstead Preparatory School is committed to ensuring that its technical infrastructure supports a safe, secure, and effective digital learning environment. The school will ensure that all policies and procedures outlined in this Online Safety Policy are implemented and that those with designated responsibilities are appropriately trained and supported.

Infrastructure and Network Security

- The school's technical systems are managed and maintained to meet current safeguarding and data protection standards, and to ensure the school complies with statutory and recommended technical requirements.
- Regular reviews and audits of technical systems are carried out to evaluate security, performance, and potential vulnerabilities.
- All servers, wireless systems, and cabling are securely located with restricted physical access.
- User access to school systems and devices is strictly controlled, and users are granted access based on role and need.

User Access and Authentication

- All users (Key Stage 2 and above) are issued with unique usernames and secure passwords.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No: 1016538) and ULT (Registered in England No: 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

- The school maintains an up-to-date register of all users, managed by the IT team.
- Users are responsible for keeping their credentials secure and must not share them.
- Administrator passwords (used by the Network Manager) must be securely stored and accessible to the Headteacher or a nominated senior leader, in case of emergency.

Licensing and Software Management

- The IT Manager is responsible for ensuring that the school maintains accurate records of software licences.
- Regular checks are conducted to reconcile the number of software installations with the number of licences held to prevent breaches of the Copyright, Designs and Patents Act 1988.

Filtering and Monitoring

- All internet access is filtered to block harmful, illegal, or inappropriate content.
- Filtering includes protection against illegal content, including child sexual abuse material, using the Internet Watch Foundation CAIC list.
- Content filtering is regularly reviewed and updated.
- The school implements differentiated filtering, providing different access levels depending on the user group (e.g., staff, pupils).
- Internet usage is logged and regularly monitored by school technical staff.
- Users are made aware of this monitoring in the Acceptable Use Agreements (AUPs).

Device and Data Security

- Appropriate and regularly tested security measures are in place to protect the school network, including:
 - Firewalls
 - Antivirus and malware protection
 - Secure configuration of routers, wireless access points, and end-user devices
- All school devices and systems are protected by up-to-date antivirus software.
- Personal data must not be transferred off-site or over the internet unless it is encrypted or securely protected, in line with the school's Data Protection Policy.

Removable Media and Software Restrictions

- The use of removable media (e.g., USB sticks, external drives, DVDs) on school devices is regulated. Staff and pupils may only use such media in accordance with the school's Acceptable Use Policies, and where necessary, files must be scanned for malware.
- Downloading and installing software or executable files on school devices is restricted and must comply with the Staff/Volunteer Acceptable Use Policy. Only authorised personnel may install new software.

- Temporary users (e.g., visitors, supply teachers, trainees) must sign the Staff/Volunteer AUP before being granted limited access to school systems.

Acceptable Use Agreements (AUPs)

- AUPs are in place for staff, volunteers, pupils, and temporary users, outlining expected behaviours and permissions relating to:
 - Use of personal and school-owned devices
 - Access to the internet and online platforms
 - Data handling and digital communication
 - Use of removable storage media
- Pupils and staff are informed of the boundaries for personal use of school devices, especially those taken off-site (e.g., 1:1 devices in Years 3–6).

Use of digital and video images

The advancement of digital technologies has created rich opportunities for teaching and learning, enabling the instant capture and use of images in the classroom and beyond. However, these same technologies carry risks when digital images are published, shared, or stored without due care. The school recognises the need to balance educational benefit with the safeguarding of pupils and the protection of personal data.

To minimise risks and support safe and responsible use of digital media:

Education and Awareness

- Staff must actively educate pupils about the risks associated with taking, using, sharing, and publishing digital images, particularly in online and social media environments.
- Pupils must be taught to understand the long-term implications of image sharing and publishing, including the potential for cyberbullying, identity misuse, and reputational damage.
- Pupils must not take or share photographs or videos of others without their explicit consent.

Parental Use of Images

- In line with ICO guidance, parents/carers may record or photograph their child at school events for personal use only.
- These images must not be shared publicly (e.g. on social media), especially if other pupils appear in them, to respect privacy and safeguarding concerns.
- Parents are requested not to comment on or tag images involving other children.

Staff Use of Images

- Staff and volunteers may take digital/video images only to support educational aims.
- These images must be taken only on school-owned devices. The use of personal equipment for this purpose is strictly prohibited.
- Images must be stored securely and deleted from the device once they have been transferred to the school network or used for their intended purpose.
- Images must not be used in any way that could be seen as embarrassing, inappropriate, or that brings the school or individuals into disrepute.

Publishing Images

- Photographs or videos used for public-facing purposes (e.g. website, newsletters, displays) will be:
 - Carefully selected
 - Used in accordance with best practice guidance
 - Only published with prior written parental consent
- Pupils' full names will never be used in association with published images.
- Pupils' work will only be published online or in print with appropriate consent from both the pupil and their parent/carer.

Data Protection

Banstead Preparatory School is committed to ensuring that all personal data is handled responsibly and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Personal data must be:

- Fairly and lawfully processed – collected with consent and for a valid reason.
- Processed for specified, explicit and legitimate purposes – not used for anything beyond the original intent.
- Adequate, relevant, and limited to what is necessary – only collect what is needed.
- Accurate and, where necessary, kept up to date – inaccuracies must be corrected promptly.
- Kept for no longer than is necessary – data must be securely deleted when no longer needed.
- Processed in a way that ensures appropriate security – including protection against unauthorised access, loss, or damage.
- Handled in accordance with the rights of the individual – including rights to access, rectify, erase, and restrict processing.
- Transferred only to countries or organisations with adequate safeguards in place – ensuring personal data is protected internationally.

Core Data Protection Principles

The school ensures that:

- It only holds the minimum personal data necessary to fulfil its functions and responsibilities.
- Personal data is not retained longer than necessary, in accordance with statutory and regulatory retention schedules.
- Every effort is made to ensure data is accurate, up to date, and that any inaccuracies are corrected promptly.
- All personal data is:
 - Fairly and lawfully obtained, in line with the school's Privacy Notice
 - Lawfully processed, in accordance with applicable Conditions for Processing

Governance and Compliance

- The school has an up-to-date and implemented Data Protection Policy.
- The school is registered as a Data Controller with the Information Commissioner's Office (ICO).
- Key responsible persons are appointed:
 - Senior Information Risk Officer (SIRO)
 - Information Asset Owners (IAOs) across relevant areas.
- Data protection risk assessments are conducted where appropriate.
- There are clearly defined procedures for:
 - Secure storage, access, and transfer of data
 - Deletion, disposal, and retention of personal data
 - Logging, reporting, and managing data breaches or security incidents
- Data subjects (e.g. pupils, parents, staff) have clearly communicated rights of access, and requests are handled in line with legal timeframes.
- Contracts involving personal data transfer to third parties contain specific Data Protection clauses.
- Use of cloud services (e.g. OneDrive, Office 365) is governed by school policy and compliant with ICO requirements.

Staff Responsibilities

All staff must ensure the following practices are consistently applied:

- Personal data must be kept secure at all times, minimising the risk of loss, misuse, or unauthorised access.
- Personal data must only be accessed on secure, password-protected devices.
- Devices must be properly locked or logged off when unattended.
- When transferring data, staff must use encrypted and password-protected school platforms, such as:
 - OneDrive (Office 365) or other approved secure channels.
- Portable storage devices (e.g. USB drives, memory sticks) are not permitted on site under any circumstances.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No: 1016538) and ULT (Registered in England No: 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

Communications

Use of School Email and Communication Systems

- The official Banstead Preparatory School email system (Office 365) is the only authorised platform for staff and pupil communication and is considered secure and monitored.
- All email and communication traffic via school systems is subject to monitoring in line with safeguarding and data protection responsibilities.
- Staff and pupils must only use school email accounts (not personal email or messaging services) for school-related communication.

Appropriate Use and Professional Standards

- All digital communication between staff and pupils or between staff and parents/carers—whether via email, virtual learning environments (VLE), chat tools, or other platforms—must be professional in tone and content.
- Whole class or group email addresses may be used for younger pupils (e.g. Key Stage 1), while individual school email addresses will be provided for pupils in Key Stage 2 and above, strictly for educational purposes.

Handling Inappropriate Communications

- Any user who receives a communication that is inappropriate, offensive, discriminatory, threatening, or makes them feel uncomfortable must report it immediately to the designated safeguarding lead or other nominated person, in line with the school's safeguarding and behaviour policies.
- Users must not reply to such messages under any circumstances.

Education and Awareness for Pupils

- Pupils will receive guidance on online safety, including:
 - The risks of sharing personal information
 - How to recognise inappropriate messages
 - Reporting procedures
 - Maintaining respectful and appropriate digital communication

Website and Staff Contact Information

- Personal information (including staff contact details) must not be posted publicly on the school website or shared inappropriately.
- Only official school email addresses will be used to identify staff members publicly or within communication systems.

Social Media – Protecting Professional Identity

Banstead Preparatory School recognises its duty of care to provide a safe and secure environment for both pupils and staff. This responsibility extends to online conduct, particularly on social media platforms. The inappropriate use of social media can expose individuals and the school to legal, reputational, and safeguarding risks.

Schools and local authorities may be held vicariously liable for the actions of employees if such actions occur during the course of employment. Therefore, staff must maintain professional boundaries at all times, both on and offline.

Measures to Minimise Risk and Protect Professional Identity

To safeguard the school community and reduce the likelihood of harm, Banstead Preparatory School implements the following measures:

- Mandatory training for staff covering:
 - Acceptable use of technology
 - Risks of social media
 - How to check and maintain privacy settings
 - Data protection responsibilities
 - How to report inappropriate activity or concerns
- Clear reporting procedures including:
 - Defined responsibilities
 - Step-by-step protocols
 - Proportionate sanctions for policy breaches
- Risk assessments to evaluate and mitigate legal or reputational risks associated with staff social media use.

Staff Responsibilities on Social Media

Staff must ensure that:

- No references are made to pupils, parents/carers, or other staff members on personal social media platforms.
- They do not engage in online discussions about personal matters related to the school community.
- Personal views and opinions expressed online must not be attributed to Banstead Preparatory School or its governing body.
- Privacy and security settings on personal social media accounts are regularly reviewed and set to the highest level to protect personal information.

Monitoring of School Social Media Usage

The school's use of social media for professional purposes (e.g. communication, promotion, community engagement) will be monitored and reviewed regularly by Head of Marketing and Admissions. Compliance with relevant policies—including the Social Media, Data Protection, Communications, and Digital Image & Video Policies—will be ensured.

Unsuitable / Inappropriate Activities

While some online activities are clearly illegal and absolutely prohibited (e.g. accessing or sharing child abuse imagery, or promoting racist content), others—though legal—are still inappropriate within the school context.

The school outlines below the types of online behaviour that are banned on school systems and also considered unacceptable outside of school when using school equipment:

Prohibited Activities Include:

- Cyberbullying or harassment
- Use of social media for inappropriate or non-professional purposes
- Accessing adult, violent, or extremist material
- Gambling or betting
- Accessing websites promoting self-harm, suicide, or eating disorders
- Using school systems for personal financial gain or business
- Misuse of copyrighted materials
- Downloading or installing unauthorised software or applications
- Bypassing or attempting to bypass the school's internet filters or security settings
- Posting or sharing confidential school information on public or personal platforms

All users (including staff, pupils, and authorised visitors) are expected to uphold the school's high standards of behaviour and professionalism in both physical and digital spaces. Breaches of this policy may result in disciplinary action, up to and including termination of employment or exclusion from school.

User Actions

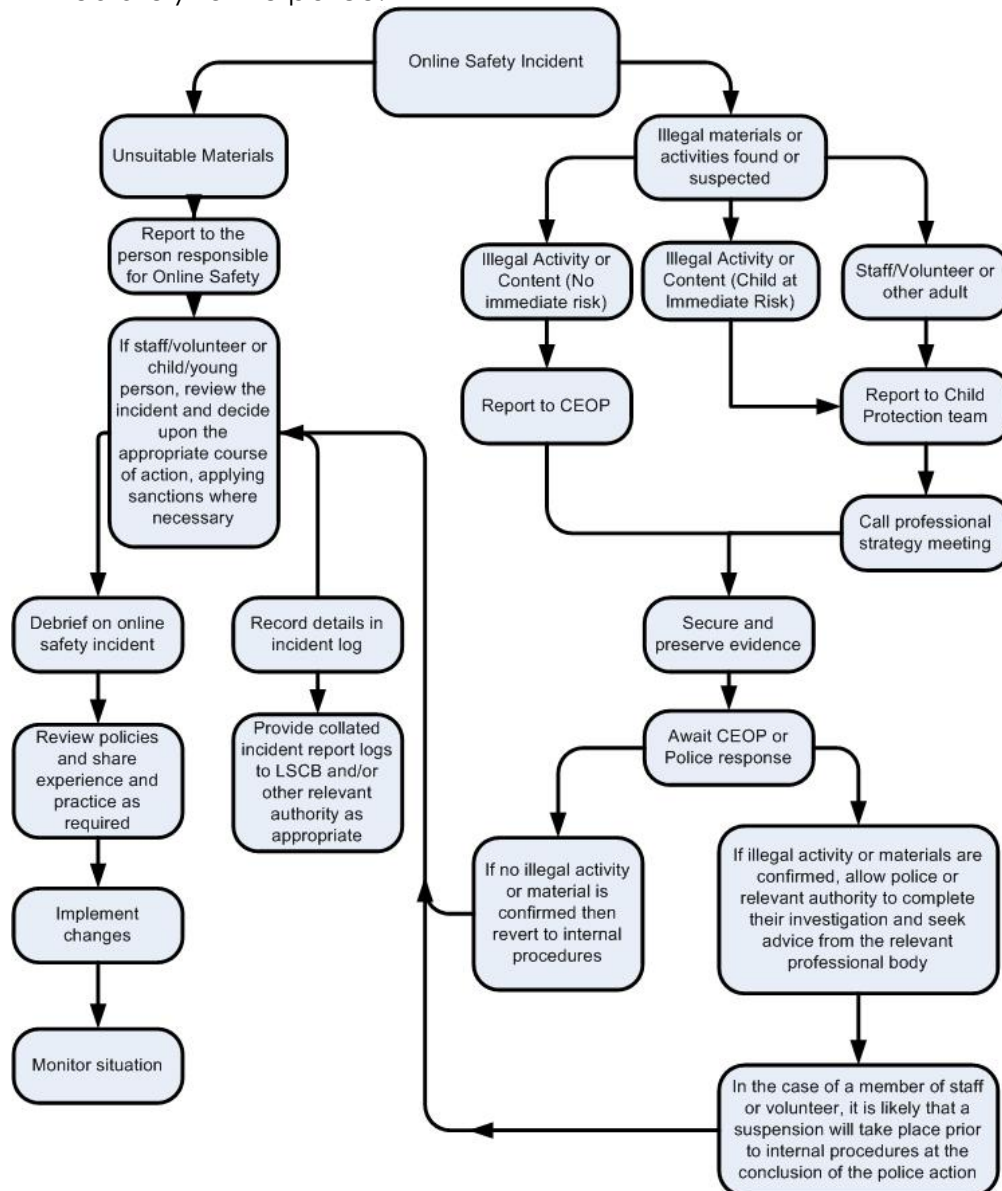
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
Pornography				X	
promotion of any kind of discrimination				X	
threatening behaviour, including promotion of physical violence or mental harm				X	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non educational)			X		
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting eg Youtube			X		

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748. Charity No. 1016538) and ULT (Registered in England No. 4439859. An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

This policy applies to all members of our school community, including those in our EYFS setting. Banstead Prep School is fully committed to ensuring that the application of this policy is non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.

Banstead Prep School seeks to implement this policy through adherence to the procedures set out in the rest of this document. In line with our Provision of Information policy, this document is available to all interested parties on our website and on request from the School Office and should be read in conjunction with the following documents: Child Protection Policy, Behaviour Management Policy, Social Media Policy and the Staff Code of Conduct.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748. Charity No. 1016538) and ULT (Registered in England No. 4439859. An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

This document is reviewed annually by the Online Safety Co-coordinator or as events or legislation change requires. The next scheduled date for review is September 2026.

Pupil Acceptable Use Policy Agreement (EYFS / Pre Prep)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- 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 / tablet or access to the internet

Child's Name:

Signed (parent):

Pupil Acceptable Use Policy Agreement (Prep)

Banstead Preparatory School Policy

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 have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

For the purposes of the following agreement, a 1:1 device issued by the school to a Year 3, 4, 5 or 6 pupil is classed as a 'school device' and not a 'personal device', as it is owned and managed by the school.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that Banstead Preparatory School will monitor my use of the systems, devices and digital communications;
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it;
- I will be aware of "stranger danger" when I am communicating on-line;
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line;
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details etc.)

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the Banstead Preparatory School systems, devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission;
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work;
- I will not use the Banstead Preparatory School systems, devices for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so;
- I will act as I expect others to act toward me;
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission;
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive, or inappropriate language and I appreciate that others may have different opinions;
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and:

- I will only use my own personal devices (mobile phones / cameras) in school if I have permission. I understand that, if I do use my own devices in Banstead Preparatory School, I will follow the rules set out in this agreement, in the same way as if I was using school equipment;
- If I need to bring my mobile phone into school, I will hand it into the office at the beginning of the school day and collect them at the end of the school day;
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials;
- I will immediately report any damage or faults involving equipment or software; however this may have happened;
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes);
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer or tablet settings without permission;
- I will not use social media sites whilst on site and/or using Banstead Preparatory School devices.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work;
- Where work is protected by copyright, I will not try to download copies (including music and videos);

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that Banstead Preparatory School will follow the behaviour policy if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information);
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school computing equipment and network / internet, as well as school sanctions in line with our behaviour policy.

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

- I use Banstead Preparatory School systems and devices (both in and out of school);
- I use my own devices in Banstead Preparatory School (when allowed) e.g. mobile phones, cameras etc.;
- I use my own equipment out of the Banstead Preparatory School in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.;
- I will not use any programmes or software that might allow me to bypass the filtering / security systems in place.

Please now use the link in the letter to complete a digital confirmation that you have read and agreed to this Acceptable Use Agreement.

Home Use Agreement (For 1:1 Devices in Years 3, 4, 5 and 6)

This document invites you to commit to the principles outlined in this Banstead Prep Home Use agreement, covering areas including what Banstead Prep will do, what we are asking you as a parent/carers to do, and what your child will be required to do.

When you have read this document, we invite you and your child to sign the agreement and return it to us. This will help to ensure that we are all working together to achieve success.

Safety arrangements

Our pupils' safety and wellbeing are our highest priority. To deter theft and to encourage careful care of the iPad, we have installed some security features and are working closely with local Police on crime prevention. Devices reported as lost or stolen will be locked by school to make them unusable, and tracked so they can be recovered.

Banstead Prep will:

- ☐ provide an iPad in a case, with charging lead and plug, to your child;
- ☐ make sure that the device is working and that repairs are dealt with as quickly and effectively as possible;
- ☐ provide technical support to aid in the use of the device in the school and where possible, when it is used away from the school;
- ☐ ensure that the iPad is protected against viruses;
- ☐ apply web filtering and monitoring software when on the internet in school;
- ☐ set the iPad to block access to the most harmful / inappropriate websites whilst in use at home;
- ☐ give students and parents / carers a detailed introduction to using the device how to care for the device and the software;
- ☐ provide ongoing technical support and maintenance when required if the device is used correctly within these terms and conditions;

As Parents/Carers we will:

- ☐ ensure that our child cares for their iPad when working at home and will not take it out of the case at any time;
- ☐ make sure the iPad is fully charged, and our child brings it to school every school day;
- ☐ support our child in remembering to leave the iPad on charge, overnight, in a communal space (not the child's bedroom);
- ☐ monitor iPad use at home to ensure the device is used appropriately.
- ☐ read the iCare Terms and Conditions;
- ☐ ensure that the iPad is maintained in good condition, and we understand that if there is a negligent loss or damage that cannot be repaired that we may be liable for the full repair or replacement cost;
- ☐ report any faults with the iPad or installed software promptly;

- ☐ make sure the iPad is not used for any illegal and/or anti-social purpose, including access to inappropriate internet sites, or social networks;
- ☐ report any loss or damage (including accidental loss or damage) promptly to the I.T. Service Desk;
- ☐ report any theft to the Police immediately and get a crime reference number that will be passed on to Banstead staff;
- ☐ Ensure that the iPad is returned when the student leaves the school for whatever reason, or at any other time upon the request of a member of school staff.

As a Student I will:

- ☐ Look after my iPad and charger very carefully;
- ☐ keep my iPad in the case that was issued to me at all times;
- ☐ make sure that my iPad is not switched with any other iPad;
- ☐ charge my iPad overnight in a communal space at home (not in my bedroom);
- ☐ make sure the battery is 100% charged at the beginning of each school day;
- ☐ always carry it to and from school in a bag and especially make sure that it is kept in a bag and out of sight on public transport;
- ☐ take care when it is transported that it is as safe as possible (e.g. cannot be seen in a vehicle; not left unattended on a bus etc.);
- ☐ make sure my iPad is not damaged by careless or deliberate actions, including anyone messing or playing around with it and using it for things it wasn't meant to be used for;
- ☐ if I think there is a problem with my device, I will report the matter promptly to my teacher;
- ☐ not write on, decorate or customise the outside of the iPad, its case, etc.;
- ☐ not leave the iPad unattended at any time unless secure either in school or at home.

Please now use the link in the letter to complete a digital confirmation that you have read and agreed to this Home Use Agreement.

Staff (and Volunteer) Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that Banstead Preparatory School will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, OneDrive etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

BANSTEAD PREPARATORY SCHOOL SUTTON LANE BANSTEAD SM7 3RA
01737 363601 OFFICE@BANSTEADPREP.COM

Banstead Prep School is part of United Learning. United Learning comprises: UCST (Registered in England No: 2780748, Charity No: 1016538) and ULT (Registered in England No. 4439859, An Exempt Charity). Companies limited by guarantee. VAT number 834 8515 12. Registered address: United Learning, Worldwide House, Thorpe Wood, Peterborough, PE3 6SB. Tel: 01832 864 444

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using Banstead Preparatory School ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website/social media) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the Banstead Preparatory School:

- When I use my mobile devices (laptops / tablets / mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using Banstead Preparatory School equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on Banstead Preparatory School systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not use or access a portable computer /USB device on site
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to Banstead Preparatory School equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Banstead Preparatory School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of Banstead Preparatory School:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Banstead Preparatory School.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date: