

THE IVORY FEDERATION

Propps Hall Junior, Infant and Nursery School
Springhead Infant and Nursery School
Rushcroft Primary School

ONLINE SAFETY, ACCEPTABLE USE & FILTERING AND MONITORING POLICY

CONTENTS

1. Filtering and Monitoring
2. Breaches
3. Incident Reporting
4. Cyber Security and Malware
5. Data Security
6. Access and Physical Security
7. Data Protection Officer (DPO)
8. Disposal of ICT Equipment and Data
9. Email and Electronic Communications
10. Online Safety and Pupils with SEND or Additional Needs
11. Online Safety – Roles and Responsibilities
12. Online Safety Education and Curriculum
13. Staff Training and Awareness
14. Internet and Network Use
15. Artificial Intelligence
16. Parental Involvement
17. Passwords and Account Security
18. Remote Access
19. School Devices and Equipment
20. Personal Devices and Mobile Phones

Appendix 1: Staff Acceptable Use Agreement

Appendix 2: Safe and Responsible Use of Technology – Rules for Pupils

Policy written August 2026

RATIONALE

Digital technology and online services are an integral part of teaching, learning and everyday life. They provide significant opportunities for communication, creativity and learning, but can also expose children and adults to potential risks.

The Ivory Federation is committed to ensuring that technology is used safely, responsibly and effectively. We recognise that online safety is an essential part of safeguarding and that children need to develop the knowledge, understanding and behaviours that enable them to navigate the online world safely and confidently.

Online safety risks may arise through content, contact, conduct and commerce and may include harmful or inappropriate content, online abuse, exploitation, bullying, misinformation, privacy and data-security risks, and the inappropriate use of emerging technologies, including generative artificial intelligence (AI).

Effective online safety is supported through education, appropriate filtering and monitoring, robust safeguarding procedures, secure use of technology and clear expectations for all members of the school community.

PURPOSE

We recognise our responsibility to educate children about online safety and to teach the knowledge, behaviours and critical thinking skills they need to use technology safely, responsibly and legally, both within and beyond school.

The Federation also recognises its responsibility to protect personal, sensitive and confidential information. All staff have a responsibility to handle information securely and in accordance with the Federation's Data Protection and Privacy Policy.

This policy, together with the Federation's Acceptable Use Agreements, applies to staff, governors, visitors and pupils and covers the use of school-provided technology, systems, networks and online services, together with personally owned devices where their use affects the school, its pupils, staff or wider community.

BROAD GUIDELINES

1. Filtering and Monitoring

The Federation has appropriate filtering and monitoring systems in place to safeguard pupils and staff when using school networks and internet-connected devices.

The governing bodies have overall strategic responsibility for ensuring that appropriate filtering and monitoring arrangements are in place. The Executive Headteacher has senior leadership responsibility for ensuring that these arrangements are implemented effectively. The Designated Safeguarding Lead (DSL) has responsibility for ensuring that safeguarding concerns identified through filtering and monitoring are responded to appropriately. Technical support is provided by the Federation's ICT support provider, Fingertip Solutions.

At Propps Hall, Smoothwall Monitor is used to provide additional monitoring of online activity. Senior leaders receive regular monitoring information and urgent alerts where potentially concerning activity is identified. The Federation intends to extend enhanced monitoring arrangements across its other schools.

Safeguarding concerns identified through filtering or monitoring will be reported to the DSL or a Deputy DSL and managed and recorded in accordance with the Federation's safeguarding procedures.

The effectiveness of the Federation's filtering and monitoring arrangements will be formally reviewed at least annually. The review will consider the current provision, identified risks, safeguarding needs, emerging technologies and whether the systems remain appropriate for the age and needs of pupils.

Appropriate checks will also be undertaken during the year to ensure that filtering and monitoring systems are operating as expected across school-managed devices and relevant locations. A record will be retained of reviews and checks undertaken and any resulting actions.

Staff will be made aware of filtering and monitoring arrangements, their responsibilities in relation to them and the process for reporting concerns as part of safeguarding and online-safety training and induction.

2. Breaches

Any breach or suspected breach of this policy will be taken seriously and responded to appropriately according to the nature and seriousness of the incident.

Where appropriate, this may include restriction or withdrawal of access to school ICT systems or equipment, action in accordance with the school's Behaviour Policy, safeguarding procedures, staff disciplinary procedures or Data Protection and Privacy Policy, and referral to external agencies where required.

Any safeguarding concern relating to the online behaviour of a child or adult must be reported immediately in accordance with the Federation's safeguarding procedures.

3. Incident Reporting

All users have a responsibility to report concerns, incidents or suspected misuse promptly.

Safeguarding concerns, including concerns arising from online activity, filtering or monitoring, must be reported immediately to the Designated Safeguarding Lead (DSL) or a Deputy DSL and recorded in accordance with the Federation's safeguarding procedures.

Suspected data breaches, loss or unauthorised disclosure of personal information, or loss or theft of equipment containing personal data must be reported immediately to the Executive Headteacher and/or Data Protection Officer (DPO) in accordance with the Federation's Data Protection and Privacy Policy.

Technical security incidents, including suspected malware, compromised accounts, unauthorised access or other cyber-security concerns, must be reported promptly to the school's ICT support provider and an appropriate senior leader.

Where an incident falls into more than one category, all relevant procedures will be followed.

4. Cyber Security and Malware

The Federation takes appropriate technical and organisational measures to protect its systems, networks and information from cyber-security threats.

The Federation works with its ICT support provider, Fingertip Solutions, to maintain appropriate cyber-security controls and follows relevant Department for Education cyber-security standards and guidance.

Security measures include, as appropriate:

- multi-factor authentication for access to school email accounts and other systems where available;
- encryption to protect school data and communications;
- appropriate firewall, filtering, monitoring, anti-virus and malware protection;
- regular security updates, software patching and maintenance;
- secure management of user accounts and access permissions;
- appropriate backup and recovery arrangements; and
- procedures for identifying, reporting and responding to suspected cyber-security incidents.

Staff must not disable or interfere with security measures installed on school equipment or systems. Passwords and authentication information must be kept secure and must not be shared.

Any suspected malware, compromised account, unauthorised access, phishing attempt or other cyber-security incident must be reported promptly to the school's ICT support provider and an appropriate senior leader.

The Federation will keep its cyber-security arrangements under review and will respond to changes in Department for Education standards, emerging risks and advice from its ICT support provider.

The Federation's three schools are members of Police CyberAlarm, supporting the Federation's wider approach to identifying and managing cyber-security threats and strengthening its resilience to cyber incidents.

5. Data Security

The Federation takes the security of personal, sensitive and confidential information seriously. All staff are responsible for handling information securely and in accordance with the Federation's Data Protection and Privacy Policy.

Staff must use only authorised systems and services for storing, accessing, sharing or transmitting school information and must follow the security measures and guidance provided by the Federation and its ICT support provider.

Any actual or suspected loss, unauthorised disclosure or compromise of personal data must be reported immediately in accordance with the Federation's data protection procedures.

6. Access and Physical Security

Access to school systems and information will be restricted according to an individual's role and responsibilities. Users must only access systems and information for which they are authorised and must take reasonable steps to prevent unauthorised access.

School-owned devices and equipment must be kept secure. Portable devices should not be left unattended in public places or visible in unattended vehicles and must be transported and stored securely.

Staff must take appropriate precautions when viewing, printing or handling personal, sensitive or confidential information. Screens should be locked when left unattended, and printed or copied confidential information should be collected promptly and stored or disposed of securely.

Any loss, theft or suspected unauthorised access to school equipment, systems or information must be reported promptly in accordance with the Federation's incident-reporting procedures.

7. Data Protection Officer (DPO)

The Federation's Data Protection Officer (DPO) service is provided by Illuminate Learning Ltd. Current contact details are available on each school's website.

The DPO provides independent advice and oversight in relation to data protection and supports the Federation in meeting its legal obligations when processing personal information.

Staff must report actual or suspected personal data breaches promptly in accordance with the Federation's Data Protection and Privacy Policy and incident-reporting procedures.

8. Disposal of ICT Equipment and Data

ICT equipment and storage media that are no longer required will be disposed of securely and in accordance with relevant legal requirements and Federation procedures.

Fingertip Solutions, the Federation's ICT support provider, manages the secure disposal of redundant ICT equipment and storage media on behalf of the Federation.

Where equipment or storage media has contained personal, sensitive or confidential information, appropriate measures will be taken to ensure that the information cannot be recovered before the equipment is reused, transferred or disposed of.

9. Email and Electronic Communications

School email and electronic communication systems are provided for professional purposes. Staff must use their school-provided email account or another authorised school communication system when conducting school business and must not use personal email accounts for school-related communication.

Communication with parents and carers will normally be undertaken through the school's designated generic email accounts or other approved school communication systems rather than individual staff email accounts. This supports appropriate professional boundaries, continuity of communication and effective management of correspondence.

Staff should not provide parents, carers or pupils with personal email addresses, telephone numbers or other personal contact details.

Communications with external organisations must be professional, appropriate and limited to information necessary for the intended purpose. The Executive Headteacher or other appropriate senior leader should be copied into correspondence where their involvement or oversight is required.

Personal, sensitive or confidential information must only be transmitted using authorised systems and in accordance with the Federation's Data Protection and Privacy Policy. Staff must take particular care to check recipients before sending information and should use appropriate secure methods where sensitive information is being shared.

Staff must remain alert to phishing, suspicious links, unexpected attachments and other potentially malicious communications and report concerns promptly in accordance with the Federation's cyber-security procedures.

School email and communication systems may be monitored where appropriate and lawful. Users should therefore have no expectation that communications made using school systems are private.

Staff must manage their school email accounts appropriately, including maintaining the security of their account and using appropriate out-of-office arrangements during extended periods of absence.

10. Online Safety and Pupils with SEND or Additional Needs

The Federation recognises that some pupils, including those with special educational needs and disabilities (SEND) or additional needs, may be more vulnerable to online risks or may require additional support to understand and apply online-safety messages.

Online-safety teaching will be adapted where appropriate to meet individual needs. This may include additional explanation, modelling, repetition, visual support, reminders or opportunities to practise safe and responsible online behaviours.

Staff will consider pupils' individual communication, social understanding and learning needs when planning the use of technology and responding to online-safety concerns.

The Federation will work with parents and carers, where appropriate, to promote consistent approaches to keeping children safe online.

11. Online Safety - Roles and Responsibilities

Online safety is an integral part of safeguarding and is a shared responsibility across the Federation.

The governing bodies have strategic oversight of online safety and are responsible for ensuring that appropriate arrangements are in place. The Executive Headteacher has overall responsibility for ensuring that this policy is implemented effectively.

Austin Pass is the Federation's Online Safety Lead and is a member of the safeguarding team. He supports the development and implementation of online-safety practice across the three schools and keeps abreast of relevant developments, risks and guidance.

The Designated Safeguarding Lead (DSL) takes lead responsibility for safeguarding and child protection, including safeguarding concerns relating to online safety. Concerns about a child's welfare arising from online activity,

filtering or monitoring must be reported to the DSL or a Deputy DSL in accordance with the Federation's safeguarding procedures.

The Federation's ICT support provider provides technical expertise and support in relation to network security, filtering, monitoring and cyber security.

Senior leaders and governors will receive appropriate information about online-safety risks, arrangements and developments to enable them to fulfil their respective responsibilities.

All staff have a responsibility to promote safe and responsible use of technology, follow the Federation's acceptable-use requirements and report concerns promptly.

12. Online Safety Education and Curriculum

Online safety is taught as part of the Federation's wider curriculum, including through Relationships, Sex and Health Education (RSHE) and Computing.

The curriculum provides age-appropriate and progressive teaching to help pupils understand how to use technology safely, responsibly and respectfully. This includes recognising and managing online risks, protecting personal information, evaluating online content, understanding appropriate online behaviour and knowing how and where to seek help.

Online-safety teaching is reinforced across the wider curriculum and through relevant assemblies, events and opportunities arising from pupils' use of technology.

Further detail about the planned progression of online-safety education is contained within the Federation's RSHE and Computing curriculum documentation.

13. Staff Training and Awareness

Staff will receive appropriate information and training about online safety, filtering and monitoring, cyber security and acceptable use as part of the Federation's safeguarding arrangements.

New staff will be made aware of this policy, the Acceptable Use Agreement and their responsibilities for online safety as part of their induction.

Staff are expected to understand their responsibilities for safeguarding pupils when using technology, to remain alert to online risks and to know how to report safeguarding, data-protection and cyber-security concerns.

Relevant updates will be provided where risks, technology, legislation or statutory guidance change.

14. Internet and Network Use

Access to the internet and school networks is provided to support teaching, learning and the effective operation of the Federation. All users are expected to use these facilities safely, responsibly and in accordance with this policy and the relevant Acceptable Use Agreement.

Pupils will have age-appropriate access to online resources under appropriate staff supervision. Staff should use professional judgement when selecting online content and resources and should ensure that their use is appropriate for the age and needs of pupils.

The Federation uses technical filtering arrangements to restrict access to inappropriate or harmful online content. Internet and network activity may be logged and monitored in accordance with the Federation's filtering and monitoring arrangements.

If a pupil or member of staff inadvertently accesses inappropriate or harmful content, they should close or minimise the content where possible and report the incident promptly. Safeguarding concerns must be reported to the DSL or a Deputy DSL in accordance with safeguarding procedures.

Users must not deliberately access, create, download, upload, store or distribute illegal, harmful, offensive or inappropriate material using school systems or equipment.

Software, applications, browser extensions or other programs must not be installed on school-managed equipment without appropriate authorisation from the Federation's ICT support provider.

The use of personally owned devices on school networks will be subject to the Federation's security and acceptable-use requirements.

15. Artificial Intelligence

The Federation recognises that artificial intelligence (AI), including generative AI, can provide useful opportunities to support teaching, learning, administration and leadership. Staff may use approved AI tools for legitimate professional purposes, subject to the expectations within this policy.

When using AI, staff must:

- use professional judgement and remain responsible for the accuracy, appropriateness and quality of any AI-generated content they use;
- check AI-generated information before relying upon or sharing it;
- not enter personal, sensitive, confidential or safeguarding information about pupils, families, staff or other individuals into publicly available or unapproved AI systems;
- comply with the Federation's data protection, safeguarding, copyright and information-security requirements;
- consider potential bias, misinformation or inappropriate content within AI-generated outputs; and
- ensure that the use of AI supports, rather than replaces, appropriate professional judgement and decision-making.

AI must not be used to make significant decisions about individual pupils or staff without appropriate human oversight and professional judgement.

Any use of AI with pupils must be age-appropriate, purposeful and appropriately supervised. Staff must consider the terms of use and age requirements of individual AI services before permitting pupils to access them.

The Federation will keep the use of AI under review as technology, associated risks and national guidance continue to develop.

16. Parental Involvement

The Federation recognises the important role of parents and carers in supporting children to use technology safely and responsibly.

Schools will provide parents and carers with appropriate information, advice and resources to support online safety at home. This may include information shared through school websites, newsletters, social media, workshops or other communications.

Parents and carers will be made aware of the school's expectations for safe and responsible use of technology and are encouraged to reinforce these expectations at home.

Appropriate consent will be sought for the use of pupils' images and other information in accordance with the Federation's procedures and Data Protection and Privacy Policy.

Where online-safety concerns affect an individual pupil, the school will work with parents and carers where appropriate as part of its safeguarding and pastoral response.

17. Passwords and Account Security

Users must take appropriate steps to protect the security of their school accounts and systems.

Users must:

- use only accounts and login credentials allocated or authorised for their use;
- keep passwords and authentication information secure and not share them with others;
- use strong passwords in accordance with the security requirements applied to school systems;
- use multi-factor authentication where this is provided;
- lock devices or screens when leaving them unattended;
- report any suspected compromise of an account or password promptly; and
- comply with any additional security requirements introduced by the Federation or its ICT support provider.

Staff must not permit another person to use their individual account or authentication credentials.

Access rights will be managed according to an individual's role and responsibilities. Accounts belonging to staff or other users who leave the Federation, or who no longer require access, will be disabled or removed promptly.

Fingertip Solutions supports the Federation in managing account security, access controls and associated technical security arrangements.

18. Remote Access

Staff may access authorised school systems remotely where this is necessary for legitimate professional purposes.

Users are responsible for maintaining the security and confidentiality of school information when working remotely and must follow the Federation's data-security and cyber-security requirements.

Staff must:

- use only authorised accounts, systems and methods of access;
- keep passwords and authentication information secure and use multi-factor authentication where provided;
- take appropriate precautions to prevent information being viewed or accessed by unauthorised individuals;
- ensure that school information is stored and shared only through authorised systems; and
- report any loss, suspected compromise or unauthorised access promptly.

School systems must not be accessed using devices or networks where doing so would present an unacceptable security risk. Staff should seek advice from Fingertip Solutions where they are unsure whether remote access is secure.

19. School Devices and Equipment

School-owned devices and ICT equipment are provided for legitimate educational and professional purposes. Users are responsible for taking reasonable care of equipment allocated to them and for using it in accordance with this policy and the relevant Acceptable Use Agreement.

School devices must be kept physically secure and should not be left unattended in public places or visible in unattended vehicles. Appropriate precautions must be taken when transporting or using devices away from school.

Users must not make unauthorised changes to school equipment or install software, applications or other programs without appropriate authorisation. Technical changes, installations and security updates will be managed or approved by Fingertip Solutions.

School information must be stored using authorised systems and services and must not be stored solely on individual devices. Devices used to access or store school information must have appropriate security measures in place.

Equipment issued to staff will be appropriately recorded. Staff must return school-owned devices and equipment when requested and on leaving the Federation.

Loss, theft, damage or suspected compromise of school equipment must be reported promptly to an appropriate senior leader and, where relevant, Fingertip Solutions.

20. Personal Devices and Mobile Phones

Staff may bring personal mobile phones and devices onto school premises but must use them in a way that maintains appropriate professional boundaries and does not interfere with their duties.

Personal mobile phones or devices must not normally be used to take photographs, video or audio recordings of pupils. Each school provides school-owned mobile phones for authorised photographs and recordings, and these should be used for this purpose.

Images or recordings of pupils must only be taken for legitimate educational or school purposes and in accordance with the Federation's safeguarding, data-protection and consent arrangements. Images and recordings must be stored, transferred and deleted appropriately using authorised school systems.

Staff must not use personal telephone numbers, messaging accounts, social-media accounts or other personal communication channels to communicate with pupils or parents/carers.

Where a personal mobile phone is exceptionally required for operational or emergency purposes, for example during an educational visit, its use must be appropriate, necessary and consistent with professional boundaries. Personal devices must not be used to store pupil information or images.

Pupil Mobile Phones

Year 6 pupils may bring a mobile phone to school where this is required for travelling to and/or from school independently. Parents/carers must agree this arrangement with the school.

On arrival at school, pupils are expected not to use their mobile phone. Phones must be handed in and will be stored securely for the duration of the school day. They will be returned to pupils at the end of the school day.

Pupils must not use personal mobile phones to take photographs, make recordings, access online content or communicate with others during the school day.

Where a pupil requires access to a mobile device for a specific medical or additional need, appropriate individual arrangements will be agreed with the school and parents/carers.

The Federation accepts no responsibility for the loss, theft or damage of personal devices brought onto school premises, except where responsibility arises under applicable law.

CONCLUSION

Through the implementation of this policy, the Federation aims to ensure that technology is used safely, responsibly and effectively and that pupils, staff and the wider school community are protected from online and digital risks.

Online safety forms an integral part of the Federation's safeguarding arrangements. The Federation will continue to respond to emerging technologies and risks and will ensure that its practice reflects relevant statutory guidance and national standards.

MONITORING AND REVIEW

The Executive Headteacher, supported by the Online Safety Lead, DSLs and ICT support provider, will monitor the implementation of this policy.

The governing bodies will maintain appropriate oversight of online safety, filtering and monitoring arrangements.

This policy will be reviewed annually and sooner where there are significant changes to legislation, statutory guidance, technology, identified risks or the Federation's systems and arrangements.

LINKED POLICIES

This policy should be read alongside relevant Federation policies and procedures, including:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Data Protection and Privacy Policy
- Relationships, Sex and Health Education Policy
- Behaviour Policy
- Anti-Bullying Policy
- Health and Safety Policy
- Home-School Agreement

APPENDIX 1

The Ivory Federation - Staff Acceptable Use Agreement

Digital technology is an important part of teaching, learning and the effective operation of the Federation. All staff have a responsibility to use technology safely, securely and professionally and to safeguard pupils, colleagues and school information.

By signing this agreement, I confirm that:

- I will use school technology, systems, accounts and online services responsibly and for legitimate professional purposes.
- I will keep passwords and authentication information secure, use multi-factor authentication where provided, lock unattended devices and take reasonable steps to prevent unauthorised access.
- I will use school-provided or authorised systems for school business and will not use personal email, telephone numbers, messaging or social-media accounts to communicate with pupils or parents/carers.
- I will handle personal, sensitive and confidential information securely and in accordance with the Federation's Data Protection and Privacy Policy.
- I will use AI responsibly for appropriate professional purposes. I will check the accuracy and suitability of AI-generated content and will not enter personal, sensitive, confidential or safeguarding information into publicly available or unapproved AI systems.
- I will not deliberately access, create, download, upload, store or distribute illegal, harmful, offensive or inappropriate content using school systems or equipment.
- I will not install software, applications or make unauthorised changes to school-managed equipment.
- I will use school-owned devices for photographs, video or audio recordings of pupils and will only create, store or share these for legitimate school purposes and in accordance with safeguarding, data-protection and consent arrangements.
- I will take reasonable care of school equipment and promptly report loss, theft, damage, suspected account compromise, phishing, malware or other cyber-security concerns.
- I understand that use of school networks, internet, email and systems may be filtered, monitored and logged where appropriate and lawful.
- I will report online safeguarding concerns immediately to the DSL or a Deputy DSL and report data breaches or cyber-security incidents in accordance with Federation procedures.
- I will respect copyright and intellectual property rights and ensure that my online activity, both in and outside school, is consistent with the standards expected of my professional role.
- I will support pupils to use technology safely, responsibly and respectfully.

I understand that failure to comply with this agreement may result in action being taken in accordance with the relevant Federation policies and procedures.

Staff Declaration

I have read and understood the Federation's Online Safety, Acceptable Use & Filtering and Monitoring Policy and agree to comply with this Acceptable Use Agreement.

Name: _____ **Signature:** _____

Job title: _____ **Date:** _____

Safe and Responsible Use of Technology

Rules for Pupils

Teachers will share and discuss these expectations with pupils, in an age-appropriate way, at the beginning of each school year and reinforce them throughout the year as appropriate.

Technology helps us to learn, create and communicate. These rules help us to keep ourselves and other people safe.

When I use technology in school:

- I will use school computers, tablets and online services for learning and only when I have permission.
- I will use my own account and keep my password private.
- I will treat other people kindly and respectfully when I am online.
- I will not deliberately look for, create or share anything that is upsetting, harmful or inappropriate.
- If I see something online that worries, upsets or confuses me, I will tell a trusted adult straight away. I know I will not be in trouble if I have seen something accidentally.
- I will not share personal information such as my address, telephone number, passwords or other private information online.
- I will not take or share photographs, videos or recordings of other people without permission.
- I will only communicate with other people online using the systems and activities approved by my school.
- I will not download or install apps, games, software or other files unless a member of staff has given me permission.
- I will think carefully about whether information I see online is reliable and remember that not everything online is true.
- I will only use artificial intelligence (AI) tools when my teacher has said that I may, and I will follow the instructions I am given.
- I will tell a trusted adult if someone contacts me online in a way that makes me feel uncomfortable or asks me to keep something secret.
- I will take care of school equipment and tell an adult if something goes wrong.
- I understand that the school may filter and monitor the technology and internet services I use to help keep everyone safe.