BOLD FUTURES

Bold Futures Federation
Staff Acceptable Use of ICT Policy

Latest Review: September 2025
Next Review Planned: September 2026

Signed:___________________________ (Policy Owner)

Print Name:_______________________

Review Date:______________________

Signed:___________________________ (Governor Approval)

Print Name:_______________________

Approval Date:____________________

POLICY CHANGE HISTORY

Version	Date	Status	Policy Owner	Governor Approval	Comment
1.0	Nov 16	APPROVED	LC	LT	
1.1	Feb 19	APPROVED	LC	SK	
1.2	Dec 20		LC		Merged social media policy and parts of E-safety policy
1.3	June 21	APPROVED	LC	MM	No changes – recently updated
1.4	May 2022	APPROVED	LC	MM	Updated with Arbor (replacement of SIMS)
1.5	April 2023	Approved	LC	RJ	Review of policy and update of communication with parent methods
1.6	May 2023		AP		Spelling and punctuation changes
1.7	May 2024	Approved	LC	RJ	Addition of AI
2.0	September 2025		LC		Update to include Bold Futures & new ICT provider

Bold Futures

Acceptable use of ICT policy - Staff

September 2015 Manual of Personnel Practice Managing and Developing Staff/Acceptable Use of ICT Resources/Model policy on staff acceptable use of ICT

Adapted by Bold Futures Federation

1.0 Introduction

Schools are encouraged to ensure that staff are given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. Schools and their staff are encouraged to make use of the resources developed by Childnet (http://www.childnet.com). Advice can also be sought from professional associations and trade unions.

The aims of this policy set out to:

- Provide guidelines that all members of the school community should follow in regard to the use of ICT-based technologies.
- Safeguard and protect all students and staff.
- Assist school staff working with students to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Provide clear expectations of behaviour and codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Ensure a clear structure to deal with online abuse such as cyberbullying which are cross referenced with other school policies is in place.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

2.0 Application

2.1 This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members.

2.2 The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SAP and Arbor), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environments and any other electronic or communication equipment used in the course of the employee or volunteer's work.

2.3 This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

3.0 Access

3.1 School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities.

3.2 Where staff have been provided with a school email address to enable them to perform their role effectively, it would not normally be used to communicate with parents and pupils unless express permission has been provided. Where staff are able to access email outside of school hours, the email facility should not routinely be used to undertake school business outside of normal office hours.

3.3 Access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system) , RAISE Online, FFT) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

3.4 Some staff may be provided with laptops and other equipment for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection. Only selected staff (teachers, admin and HLTA) will be able to access the school systems remotely.

3.5 Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents or carers (this will be gathered as part of the school agreement form when their child joins the school and held on Arbor) and that the school's policy in relation to use of pictures, is followed. Pupils' full names will not be used anywhere on a website, particularly in association with photographs/videos.

3.6 Schools within the federation do not provide staff with a school mobile phone and therefore staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

3.7 No mobile telephones or similar devices, even those with hands free facilities, should be used whilst driving on school business.

3.8 Access to the school telephone system for personal use should only be used in exceptional circumstances when permission has been gained by a member of SLT. Where such use is made of this facility, it must be done during break periods, and must not be excessive.

3.9 The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

4.0 Communication with parents, pupils and governors

4.1 The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. The school must indicate to staff if any other staff are permitted to make contact using the systems below:

4.1.1 School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or a home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a member of the teaching staff where they feel they need to make a telephone call to a parent.

4.1.2 Text System (Arbor in app messaging) – office staff and SLT. Where other staff need to send a message, this is normally approved by a member of the senior leadership team.

4.1.3 Letters (sent through Arbor or Google forms if permission required) – normally all teachers may send letters home, but they may be required to have these approved by the Headteacher/ Deputy Headteacher before sending. Where office staff send letters home, these will normally require approval by the Headteacher/ Deputy Headteacher.

4.1.4 Email – school email accounts should not be used for communication with parents unless approved by Headteacher/ Deputy Headteacher. If a situation of direct contact does occur, parents should be redirected to the generic office email for the school.

Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

4.2 Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils. If a member of staff needs to contact a pupil direct via any of these methods, this must be approved by the Headteacher.

4.3 Where pupils are submitting work electronically to school staff, this must be undertaken using the office email and not via personal email.

5.0 Social Media

5.1 School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

5.2 Staff should refer to Appendix 1 and the Social Media Policy which contains detailed advice on the expectations of staff when using social media.

6.0 Unacceptable Use

6.1 Appendix 2 provides a list of Do's and Don'ts for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment (an alternative reduced version will be viewed by supply teachers). School systems and resources must not be used under any circumstances for the following purposes:

6.1.1 To communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share.

6.1.2 To present any personal views and opinions as the views of the school or to make any comments that are libellous, slanderous, false or misrepresent others.

6.1.3 To access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material.

6.1.4 To communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally.

6.1.5 To communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils.

6.1.6 To upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.

6.1.7 To collect or store personal information about others without direct reference to The Data Protection Act.

6.1.8 To use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project.

6.1.9 To visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the school.

6.1.10 To undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people.

- 6.2 Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. Contact with the police will occur if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the senior leadership team or ICT lead if applicable.

6.3 Where an individual accidentally or unintentionally accesses a website or material that contains any prohibited content, they must leave the site immediately and inform the Headteacher or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated as a breach of this policy.

6.4 Where an individual has been communicated with in a manner outlined above (e.g. has received an inappropriate email or attachment), they are advised to report this immediately to the Headteacher or another member of the senior leadership team so that this can be dealt with appropriately.

Appendix 6 contains an agreement which is signed by staff in regards to acceptable use of Arbor in regards to GDPR for all staff members.

<u>Responding to incidents of misuse</u>

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. To minimise incidents of misuse, all members of the school community will understand the following responses may occur:

- Support is actively sought from other agencies as needed (e.g. the local authority, UK Safer Internet Centre helpline) in dealing with E-safety issues
- Monitoring and reporting of E-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school.
- Parents/carers are specifically informed of E-safety incidents involving young people for whom they are responsible.
- Contact with the police will occur if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

7.0 Personal and private use

7.1 All school staff with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

7.1.1 Taking place at the expense of contracted working hours (i.e. is not taking place during paid working time).

7.1.2 Interfering with the individual's work.

7.1.3 Relating to a personal business interest.

7.1.4 Involving the use of news groups, chat lines or similar social networking services.

7.1.5 At a cost to the school.

7.1.6 Detrimental to the education or welfare of pupils at the school.

7.2 Excessive personal use of school facilities is likely to be considered to be a disciplinary matter, may lead to restricted access to computer equipment and where costs are incurred (e.g. personal telephone use), the school will seek reimbursement from the member of staff.

7.3 It is important for staff to also be aware that inappropriate use of their own personal or other ICT facilities in their personal time, can have implications for their employment situation where this becomes known and the activities that are undertaken are inconsistent with the expectations of staff working with children and young people.

7.4 Where school staff have brought their own personal equipment such as mobile telephones, digital assistants, laptops and cameras into the school, these personal items should not be used during pupil contact sessions unless authorised. Staff should follow all points outlined in this section in relation to their personal use. Staff should ensure that there is no inappropriate content on any of these pieces of equipment and ensure that they are not accessed by pupils at any time. Such equipment should not normally be required to enable staff to undertake their role but where it is used, staff should take care to ensure any school data/images are deleted following use of the equipment.

7.5 Whilst individuals may be required to use their personal mobile telephone to make contact with the school, staff should exercise care as outlined in section 3.

8.0 Security and confidentiality

8.1 Any concerns about the security of the ICT system should be raised with a member of the senior leadership team.

8.2 Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords. All staff are required to log off/ lock a device when finished. If a device is found logged in, staff must log off and enter their own password before use.

8.3 School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT leader.

8.4 Where staff are permitted to work on material at home and bring it in to upload to the school server through their memory pens, they must ensure that they have undertaken appropriate virus checking on their systems. Staff should be extremely wary of any data carried on memory pens and where their use is essential, only memory pens which are password protected should be used. Where provided, staff should normally use their school issued laptop for such work.

8.5 Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the student resource pool and/or for use by staff to the teacher resource pool and/or media share.

8.6 Whilst any members of school staff may be involved in drafting material for the school website, final uploading must be completed by office staff, headteacher or ICT leader.

8.7 The school have nominated Harrap who are responsible for ensuring that all equipment is regularly updated with new software, including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify office staff, the headteacher or the ICT leader when reporting any concerns regarding potential viruses, inappropriate software or licences (this will then be passed onto Harrap).

8.8 Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

8.9 Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of copyright through their use of ICT facilities.

Appendix 3 outlines the roles and responsibilities of staff members in regards to ICT use and e-safety procedures.

9.0 Monitoring

9.1 The school uses Hampshire County Council's ICT services and is therefore required to comply with their email, internet and intranet policies.

9.2 The school and County Council reserve the right to monitor the use of email, internet and intranet communications and where necessary, data may be accessed or intercepted in the following circumstances:

9.2.1 To ensure that the security of the school and County Council's hardware, software, networks and systems are not compromised.

9.2.2 To prevent or detect crime or unauthorised use of the school or County Council's hardware, software, networks or systems.

9.2.3 To gain access to communications where necessary or where a user is absent from work.

9.3 Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or County Council may track the history of the internet sites that have been visited.

9.4 To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Hampshire County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

10.0 Whistleblowing and cyberbullying

10.1 Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephone use, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the headteacher to such abuse. Where a concern relates to the headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

10.2 It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their headteacher if they are subject to such circumstances. Advice can also be sought from professional associations and trade unions. Support is also available through Hampshire's confidential counselling service, Employee Support (0800 030 5182) and also via the UK Safer Internet Centre helpline@safetinternet.otg.uk or 0844 381 4772.

10.3 Further advice on cyberbullying and harassment can be found on Cyber bullying: Practical Advice for School Staff (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf). Alternatively, this can be accessed via the TDrive under Curriculum/ Computing.

11.0 Signature

11.1 Staff are expected to read and confirm that they have had access to the Acceptable Use Policy and that they accept and will follow its terms.

11.2 Staff must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules which may lead to a disciplinary sanction (e.g. warning), dismissal, and/or withdrawal of access to ICT facilities. Staff should be aware that in certain instances, inappropriate use of ICT may become a matter for police or social care investigations.

12.0 Data Protection Act

Schools, Local Education Authorities (LAs), the Department for Education and Skills (DCSF - the government department which deals with education), the Qualifications and Curriculum Authority (QCA), Ofsted, and the Learning and Skills Council (LSC) all process information on pupils in order to run the education system and in doing so, must comply with the Data Protection Act 1998. This means, among other things, that the data held about pupils must only be used for specific purposes allowed by law. We are therefore writing to tell you about the types of data held, why that data is held, and to whom it may be passed on.

The **school** holds information on pupils in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the school as a whole is doing. This information includes contact details, National Curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs, and any relevant medical information. From time-to-time schools are required to pass on some of this data to LEAs, the DCSF and agencies such as QCA, Ofsted and LSC that are prescribed by law.

The **Local Education Authority** uses information about pupils to carry out specific functions for which it is responsible, such as the assessment of any special educational needs the pupil may have. It also uses the information to derive statistics to inform decisions on (for example) the funding of schools, and to assess the performance of schools and set targets for them. The statistics are used in such a way that individual pupils cannot be identified from them.

Ofsted uses information about the progress and performance of pupils to help inspectors evaluate the work of schools, to assist schools in their self-evaluation, and as part of Ofsted's assessment of the effectiveness of education initiatives and policy. Inspection reports do not identify individual pupils.

The **Department for Education and Skills** (DCSF) uses information about pupils for research and statistical purposes, to inform, influence and improve education policy and to monitor the performance of the education service as a whole. The DCSF will feed back to LAs and schools information about their pupils for a variety of purposes that will include data checking exercises, use in self-evaluation analyses and where information is missing because it was not passed on by a former school. The DCSF will also provide Ofsted with pupil level data for use in school inspection. Where relevant, pupil information may also be shared with post 16 learning institutions to minimise the administrative burden on application for a course and to aid the preparation of learning plans.

Pupil information may be matched with other data sources that the Department holds in order to model and monitor pupils' educational progression; and to provide comprehensive information back to LAs and learning institutions to support their day-to-day business. The DCSF may also use contact details from these sources to obtain samples for statistical surveys: these surveys may be carried out by research agencies working under contract to the Department, and participation in such surveys is usually voluntary. The Department may also match data from these sources to data obtained from statistical surveys.

Pupil data may also be shared with other Government Departments and Agencies (including the Office for National Statistics) for statistical or research purposes only. In all these cases, the matching will require that individualised data is used in the processing operation, but that data will not be processed in such a way that it supports measures or decisions relating to particular individuals, or identifies individuals in any results. This data sharing will be approved and controlled by the Department's Chief Statistician.

The DCSF may also disclose individual pupil information to independent researchers into the educational achievements of pupils who have a legitimate need for it for their research, but each case will be determined on its merits and subject to the approval of the Department's Chief Statistician.

Pupils, as data subjects, have certain rights under the Data Protection Act, including a general right of access to personal data held on them. If you wish to access your personal data, or you wish your parents to do so on your behalf, then please contact the relevant organisation in writing; this will be your school.

Ofsted's Data Protection Officer at Alexandra House, 33 Kingsway, London WC2B 6SE

LSC's Data Protection Officer at Cheylesmore House, Quinton Road, Coventry,
Warwickshire CV1 2WT

The DCSF's Data Protection Officer at DCSF, Caxton House, Tothill Street, London, SW1H 9NA.

In order to fulfil their responsibilities under the Act the organisation may, before responding to this request, seek proof of the requestor's identity and any further information required to locate the information requested.

Separately from the Data Protection Act, regulations provide a pupil's parent (regardless of the age of the pupil) with the right to view, or to have a copy of, their child's educational record at the school. If you wish to exercise this right you should write to the school.

Data Protection Policy

School Compliance

The terms of the 1998 Data Protection Act, and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.

Advice and guidance supplied in the ***Data Protection Advice for Schools*** flyer and ***Data Protection Guidance for Schools*** booklet.

Information and guidance displayed on the Information Commissioner's website (***www.dataprotection.gov.uk***).

This policy should be used in conjunction with the school's ***Dta Protection GDPR policy***.

Data Gathering

- All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act.
- Only relevant personal data may be collected and the person from whom it is collected should be informed of the data's intended use and any possible disclosures of the information that may be made.

Data Storage

- Personal data will be stored in a secure and safe manner.
- Electronic data will be protected by standard password and firewall systems operated by the school.
- Computer workstations in administrative areas will be positioned so that they are not visible to casual observers waiting either in the office or at the reception hatch.
- Manual data will be stored where it not accessible to anyone who does not have a legitimate reason to view or process that data.
- Particular attention will be paid to the need for security of sensitive personal data.

Data Checking

- The school will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.
- Any errors discovered would be rectified and, if the incorrect information has been disclosed to

Data Disclosures

- Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.
- When requests to disclose personal data are received by telephone, it is the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.
- If a personal request is made for personal data to be disclosed, it is again the responsibility of the school to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.
- Requests from parents or children for printed lists of the names of children in particular classes, which are frequently sought at Christmas, should be politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the pupils are present in class will resolve the problem.)
- Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
- Routine consent issues will be incorporated into the school's pupil data gathering sheets to avoid the need for frequent, similar requests for consent being made by the school.
- Personal data will only be disclosed to Police Officers if they display a legitimate need to have access to specific personal data.
- A record should be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

Subject Access Requests

- If the school receives a written request from a data subject to see any or all personal data that the school holds about them, this should be treated as a Subject Access Request and the school will respond within the 40-day deadline.
- Informal requests to view or have copies or personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the school will comply with its duty to respond within the 40-day time limit.
- This policy will be included in the Policy File.
- Data Protection statements will be included in the school prospectus and on any forms that are used to collect personal data.

Use of Artificial Intelligence

1. Use of AI by Students

- Students are not permitted to use AI tools to complete their homework or any other assignments. Homework is an essential part of the learning process and should reflect the student's own understanding and effort.
- Students are encouraged to develop their problem-solving skills, creativity, and critical thinking by working independently on their assignments.
- Any use of AI for learning purposes must be supervised and approved by a teacher. This includes educational software or tools that incorporate AI to enhance learning experiences.

2. Use of AI by Teachers

- Teachers may use AI tools at their discretion to aid in lesson planning, administrative tasks, or to enhance classroom activities.
- All materials generated by AI tools must be thoroughly reviewed and verified by a teacher to ensure accuracy and appropriateness before being used in the classroom or shared with students.
- Teachers should maintain transparency with students about the use of AI tools in the classroom and promote discussions about the ethical use of AI in education.

3. Ethical Considerations and Data Privacy

- All users must respect data privacy and confidentiality when using AI tools. Personal data should not be inputted into AI systems without proper consent and understanding of how the data will be used.
- The use of AI should align with the school's values and educational goals, promoting fairness, inclusivity, and respect for all individuals.

4. Training and Support

- The federation will provide training and support for staff to effectively and responsibly use AI tools in their professional roles.
- Students will receive guidance on the ethical implications of AI and how it can be used responsibly in various contexts.

5. Monitoring and Compliance

- The school will monitor the use of AI tools to ensure compliance with this policy. Any misuse of AI by students or staff will be addressed promptly and appropriately.
- Violations of this policy may result in disciplinary action in accordance with the school's behaviour management policies.

Appendix 1: Professional Guidance and Policy on Social Networking

Pupil and Teacher Safeguarding

As a general rule, you should exercise caution when it comes to communicating with pupils and former pupils using the internet or mobiles.

For example, you should only use official school email accounts or virtual learning platforms to talk to current pupils online so that any communication is logged.

You should also only communicate on school matters as personal communication could be considered inappropriate and in breach of your professional code of conduct.

As the boundaries between the online and offline worlds blur, your pupils or parents may try to include you in their "friends" list on their online social network or get hold of your personal email address or mobile number. This could be harmless but it's important that you keep a professional distance online, just as you would in the offline world, and not include them as "friends".

If you have a mobile with Bluetooth technology, you could be at risk of "Bluejacking" (where another Bluetooth user in your vicinity can send you a message without knowing your number) or "Bluesnarfing" (where another Bluetooth user can access your mobile and steal things like your contact list, emails, texts and photos).

Ultimately, email or phone communications between you and a pupil or parent that are deemed to fall outside of agreed school guidelines might lead to disciplinary action or a criminal investigation.

Here are a few tips to help you stay in control:

- Keep your personal email address, Instant Messenger ID, mobile number and social networking ID private and don't use them for communications with your pupils or parents.
- If your Bluetooth is not switched off by default, switch it off and set it to refuse connections when you are at work.
- If, despite your best efforts, your personal contact details fall into the wrong hands and a pupil makes contact with you, let a senior manager know immediately.
- If calls or texts to your mobile are persistent, let your mobile network provider know too so that they can investigate and take the appropriate action.
- If you receive anonymous emails, IMs or messages on your social networking profile that you think could be from a pupil or parent- or if you feel you are being harassed or bullied online - report it to a senior manager and contact your internet service or social networking provider so that they can investigate and take the appropriate action.

Cyber-bullying: Guidance Document for Pupils and Parents

Do -

- Keep your passwords confidential
- Ensure you familiarise yourself with the school's policy for acceptable use of technology, the internet and email.

- Avoid the use of social networking sites whilst at school.
- Ensure that you understand how any site you use operates and therefore the risks associated with using the site
- Consider carefully who you accept as friends on a social networking site
- Report to your line manager any incidents where a pupil has sought to become your friend through a social networking site
- Check what images and information is held about you online but undertaking periodic searches of social networking sites and using internet search engines
- Take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain
- Be aware that any off-duty inappropriate conduct, including publication of inappropriate images and material and inappropriate use of technology could lead to disciplinary action
- Take screen prints and retain text messages, emails or voice mail messages as evidence
- Follow school procedures for contacting parents and/or pupils
- Only contact pupils and/or parents via school-based computer systems
- Keep your mobile phone secure at all times
- Use a school mobile phone where contact with parents and/or pupils has to be made via a mobile (e.g. during an educational visit off site)
- Erase any parent or pupil data that is stored on a school mobile phone after use
- Seek support from your manager, professional association/trade union, friend, employee support line as necessary
- Report all incidents of cyberbullying arising out of your employment to your line manager
- Report any specific incident on a Violent Incident Report (VIR) form as appropriate
- Provide a copy of the evidence with your line manager when you report it and further evidence if further incidents arise
- Seek to have offensive online material removed through contact with the site
- Report any threatening or intimidating behaviour to the police for them to investigate
- Support colleagues who are subject to cyberbullying

DON'T

- Allow any cyberbullying to continue by ignoring it and hoping it will go away
- Seek to return emails, telephone calls or messages or retaliate personally to the bullying

- Put information or images on-line, take information into school, or share them with colleagues, pupils or parents (either on site or off site) when the nature of the material may be controversial
- Accept friendship requests from pupils or parents
- Release your private e-mail address, private phone number or social networking site details to pupils and parents
- Use your mobile phone or personal e-mail address to contact parents and/or pupils
- Release electronically any personal information about pupils except when reporting to parents
- Pretend to be someone else when using electronic communication
- Take pictures of pupils with school equipment without parental permission
- Take pictures of pupils on your own equipment

Appendix 2: Roles and responsibilities

Governors

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leadership team (SLT)

- The Head teacher is responsible for ensuring the safety (including E-safety) of members of the school community, though the day-to-day responsibility for E-safety will be delegated to the E-Safety Co-ordinator (ICT manager)
- The Head teacher is responsible for ensuring that the E- Safety Co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their E-safety roles and to train other colleagues, as relevant
- The Head teacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. *This is to provide a safety net and also support to those colleagues who take on important monitoring roles*
- The Senior Leadership Team will receive regular monitoring reports from the E-safety Co-ordinator
- The Head teacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff.

E-safety Co-ordinator (ICT/ Computing leader/ DSL)

- To lead day to day responsibility for E-safety issues.
- To promote an awareness and commitment to E-safeguarding throughout the school community.
- To ensure that E-safety education is embedded across the curriculum.

- To oversee the delivery of the E-safety element of the Computing curriculum.
- To liaises with the school's designated ICT technical staff (AGILE).
- To communicate regularly with SLT and the designated E-safety Governor to discuss current issues, review incident logs and filtering.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an E-safety incident.
- To ensure that an E-safety incident log is kept up to date.
- To facilitate training and advice for all staff.
- To liaises with the Local Authority and relevant agencies.
- To keep regularly updated in E-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying and use of social media

ICT Technician (Harrap)

- To ensure that users may only access the school's networks through a properly enforced password protection policy.
- To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date).
- To ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices.
- To ensure the school's policy on web filtering is applied and updated on a regular basis (Hampshire County Council).
- To keep up to date with the school's E-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- To ensure that the use of the network/remote access /email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Co-ordinator/Headteacher for investigation.
- To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To keep up-to-date documentation of the school's e-security and technical procedures.
- To ensure that monitoring software/systems are implemented and updated as agreed in school policies.

Teaching and support staff

- To ensure they have an up-to-date awareness of E-safety matters and of the current school E-safety policy and practices.
- To ensure they know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.
- To ensure they are aware of E-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- To maintain an awareness of current E-safety issues and guidance e.g. through CPD.
- To ensure E-safety issues are embedded in all aspects of the curriculum and other school activities.
- To supervise, monitor and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant).
- To ensure that their pupils are fully aware of research skills, appropriate search engines and are fully aware of legal issues relating to electronic content including the need to avoid plagiarism and uphold copyright regulations.
- To read, understand and help promote the school's E-safety policies and guidance.
- To read, understand, sign and adhere to the school staff Acceptable ICT Use Policy.
- To be aware of E-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices.
- To report any suspected misuse or problem to the E-safety coordinator/ Headteacher to investigate.
- To model safe, responsible and professional behaviours in their own use of technology.
- To ensure that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- To ensure that any digital communications with pupils is on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Office staff

- To ensure that all data held on pupils on the school office machines have appropriate access controls in place

Appendix 3: Do's and Don'ts: Advice for Staff

Whilst the wide range of ICT systems and resources available to staff both in school and outside of school have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately, if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don'ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do

- Ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources.
- Ensure that where a password is required for access to a system, that it is not inappropriately disclosed.
- Respect copyright and intellectual property rights.
- Ensure that you have approval for any personal use of the school's ICT resources and facilities.
- Be aware that the school's systems will be monitored and recorded to ensure policy compliance.
- Ensure you comply with the requirements of the data protection act when using personal data.
- Seek approval before taking personal data off of the school site.
- Ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely.
- Report any suspected misuse or concerns that you have regarding the school's systems, resources and equipment to the headteacher or designated manager and/or designated safeguarding lead as appropriate.
- Be aware that a breach of your school's acceptable use policy will be a disciplinary matter and, in some cases, may lead to dismissal.
- Ensure that any equipment provided for use at home is not accessed by anyone not approved to use it.
- Ensure that you have received adequate training in ICT.
- Ensure that your use of ICT bears due regard to your personal health and safety and that of others.

Don't

- Access or use any systems, resources or equipment without being sure that you have permission to do so.

- Access or use any systems or resources or equipment for any purpose that you don’t have permission to use the system, resources or equipment for.
- Compromise any confidentiality requirements in relation to material and resources accessed through ICT systems.
- Use systems, resources or equipment for personal use without having approval to do so.
- Use other people’s log on and password details to access school systems and resources.
- Download, upload or install any hardware or software without approval.
- Use unsecure removable storage devices to store personal data.
- Use school systems for personal financial gain, gambling, political activity or advertising.
- Communicate with parents and pupils outside normal working hours unless absolutely necessary.

Use of email, the internet, VLEs and school and HCC intranets

Do

- Alert your Headteacher or designated manager if you receive inappropriate content via email.
- Be aware that the school’s email system will be monitored and recorded to ensure policy compliance.
- Ensure that your email communications are compatible with your professional role.
- Give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate.
- Be aware that the school may intercept emails where it believes that there is inappropriate use.
- Seek support to block spam.
- Alert your Headteacher or designated manager if you accidentally access a website with inappropriate content.
- Be aware that a website log is recorded by the school and will be monitored to ensure policy compliance.
- Answer email messages from pupils and parents within your directed time.
- Mark personal emails by typing ‘Personal/Private’ within the subject header line.

Don’t

- Send via email or download from email, any inappropriate content.
- Send messages that could be misinterpreted or misunderstood.
- Use personal email addresses to communicate with pupils or parents.
- Send messages in the heat of the moment.
- Send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude.
- Use email systems to communicate with parents or pupils unless approved to do so.
- Download attachments from emails without being sure of the security and content of the attachment.

- Forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention.
- Access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet.
- Upload any material onto the school website that doesn't meet style requirements and without approval.

Use of telephones, mobile telephones and instant messaging

Do

- Ensure that your communications are compatible with your professional role.
- Ensure that you comply with your school's policy on use of personal mobile telephones.
- Ensure that you reimburse your school for personal telephone calls as required.
- Use school mobile telephones when on educational visits.

Don't

- Send messages that could be misinterpreted or misunderstood.
- Excessively use the school's telephone system for personal calls.
- Use personal or school mobile telephones when driving.
- Use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school.

Use of cameras and recording equipment

Do

- Ensure that material recorded is for educational purposes only.
- Ensure that where recording equipment is to be used, approval has been given to do so.
- Ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy.
- Ensure that parental consent has been given before you take pictures of school pupils.

Don't

- Bring personal recording equipment into school without the prior approval of the Headteacher.
- Inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded.

Use of social networking sites

Do

- Ensure that you understand how any site you use operates and therefore the risks associated with using the site.

- Familiarise yourself with the processes for reporting misuse of the site.
- Consider carefully who you accept as friends on a social networking site.
- Report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site.
- Take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain.
- Ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page.
- Follow school procedures for contacting parents and/or pupils.
- Only contact pupils and/or parents via school-based computer systems.
- Through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role).

Don't

- Spend excessive time utilising social networking sites while at work.
- Accept friendship requests from pupils or parents – you may be giving them access to personal information, and allowing them to contact you inappropriately.
- Put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial.
- Post anything that may be interpreted as slanderous towards colleagues, pupils or parents.
- Use social networking sites to contact parents and/or pupils.

Appendix 4 : Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct.
Staff should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification if needed.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted
- I understand that it I am unable to communicate information which is confidential to the school or which I do not have the authority to share
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance
- I understand the level of authority required to communicate with parents and pupils using the various methods of communication
- I understand that I must not use the school ICT system to access inappropriate content
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission
- I will follow the school's policy in respect of downloading and uploading of information and material
- I will ensure that personal data is stored securely and is used appropriately whether in school, taken off the school premises or accessed remotely. I will not routinely keep personal data on removable storage devices. Where personal data is required, it will be password protected/encrypted and removed after use.
- I will respect copyright, intellectual property and data protection rights
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors

- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging are compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.
- I understand that inappropriate use of personal and other non-school based ICT facilities can have implications for my employment at the school where this becomes known and that activities undertaken are inconsistent with expectations of staff working with children The school may exercise its right to monitor the use of the school's ICT systems and accesses, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's ICT systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, images or sound.

Appendix 5: Supply/ visitor Code of Conduct for ICT

To ensure that visitors to the school are fully aware of their professional responsibilities when using information systems and when communicating with parents, pupils and others, they are asked to sign this code of conduct *(supply laptop sign out sheet).*

Visitors should consult the detail of the school's Policy for Staff Acceptable Use of ICT for further information and clarification if they feel it is required.

- I appreciate that ICT includes a wide range of system, including mobile phones, personal digital assistants, cameras, email, internet and HCC intranet access and use of social networking and that ICT use may also include personal ICT devices when used for school business
- I understand that it may be a criminal offence to use the school ICT system for a purpose not permitted
- I understand that school information systems and hardware may not be used for personal or private without the permission of the Headteacher
- I understand that my use of school information systems, internet and email may be monitored and recorded, subject to the safeguards outlined in the policy to ensure policy compliance
- I understand that I should seek guidance from a member of teaching staff/ SLT before contacting parents or carers

- I understand that I must not use the school ICT system to access inappropriate content
- I understand that accessing, viewing, communicating and downloading material which is pornographic, offensive, defamatory, derogatory, harassing or bullying is inappropriate use of ICT
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission
- I will follow the school's policy in respect of downloading and uploading of information and material
- I will respect copyright, intellectual property and data protection rights
- I understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidences of concern regarding children's safety to the Designated Safeguarding Lead or Headteacher.
- I will report any incidences of inappropriate use or abuse of ICT and inappropriate electronic communications, whether by pupils or colleagues, to the Headteacher, or if appropriate, the Chair of Governors
- I will ensure that any electronic communication undertaken on behalf of the school, including email and instant messaging, is compatible with my professional role and that messages do not present personal views or opinions and cannot be misunderstood or misinterpreted
- I understand the school's stance on use of social networking and given my professional role working with children, will exercise care in any personal use of social networking sites
- I will ensure that any electronic communications with pupils, where permitted, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote E-safety with pupils in my care and help them to develop a responsible attitude to system use, communication and publishing.

Appendix 6: Acceptable use of Arbor

Use of Arbor should take into consideration all of the school's policies which relate to safeguarding and data protection.

Training on acceptable use of Arbor is given to all appropriate staff.

Monitoring of Arbor, including access arrangements, is completed by the Head of School and Business Manager as required – including, but not limited to, the employment and end of employment of staff.