Ashford Church of England Primary School

2022/23

ACCEPTABLE INTERNET & E-SAFETY USE
CONDUCT FOR STAFF, THIRD PARTY STAFF, VOLUNTEERS Including PTA TRUSTEEs AND GOVERNORS

This policy applies to all persons within the school organisation who may at any time have access to school technology or network or email.

ACCEPTABLE INTERNET & E-SAFETY USE

- Private use of the internet may only take place outside of teaching/school hours (professional development activities are not deemed private). However, the school computers may not be used for the purpose of social networking unless authorised school activity/promotion.
- Receiving questionable material or chancing upon an undesirable website should notify the Head of School/School Business Manager (SBM) immediately.
- Emails sent to an external organisation should be written carefully and checked before sending in the same way as a letter written on school headed paper. **Avoid the autofill of contacts facility and check recipients before sending to ensure information remains secure, including if email addresses should be entered into the cc or bcc field**. If use of autofill results in breaches of data protection this facility will be disabled.
- Encrypt or Pin protect any document containing sensitive information before sending it to any recipient. Agree the PIN code via another communication method – phone, text as appropriate.
- Keep personal details safe and do not give them out over the internet or phone.
- Everyone should develop and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
- Only the schools approved Internet service Provider (ISP) – RM SafetyNet, should be used for school internet use.
- Change school passwords every half term to a “strong” password which includes capitals, lower case, numbers and symbols and should contain at least 8 characters.
- Ensure that the password auto-save function is turned off.
- Ensure that you are only one knows and uses your user Account and understand that anything undertaken while you are logged in, you will be held responsible for.

Lock your computer whenever you leave it unattended.

- Report any suspicious emails, I before clicking on any links, downloading any attachments or entering your user details. When you report it, do not forward the email but send a screen shot.
- Ensure that personal data is kept secure and is used appropriately, whether in the office, or when working remotely. Personal data should be stored on the on the school server or on the school SharePoint

UNACCEPTABLE USE OF THE INTERNET

- It is not acceptable to access, transmit or create any offensive, obscene or indecent images, sounds, data or other material, as well as material that is defamatory, violent, abusive, racist, homophobic or that may cause needless anxiety.
- Bringing the name of the school into disrepute.
- Breach of confidentiality that results in information being inappropriately made available to others, including through social networking sites used from phones and home computers.
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions Data Protection Legislation
- Transmission of commercial or advertising material or access to gambling websites.

- Violate the Data Protection Act 2018 by deliberately corrupting or destroying other users' data or violating privacy of others.
- Disrupting the work of others or wasting the time of staff or other users.
- Do not upload a photo to your email profile.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Executive Head/Head of School will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities. Staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies.

ACCESS TO SCHOOL ICT FACILITIES AND MATERIALS

The school's SBM and ICT Provider manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other mobile devices
- Access permissions for certain programmes or files
- Use of copier facilities
- The school's filtering and monitoring will be reviewed regularly, and details of blocked searches will be reported at DSL meetings and to the Full Governing Body in line with advice in KCSIE 2022.

Personal use of ICT facilities including copying must not be overused or abused.

Only devices supplied by the school should be used to access the school network, as they will have the required level of security and protection. Authorised users will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities. One User, One Login. Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the SBM.

USE OF EMAIL

- The school provides each member of staff, Governors and the PTA with an email address. This email account should be used for school purposes only. Unless with the specific agreement of the SBM or Head of School.
- Governors should use the agreed SharePoint file for sharing documents and information in relation to their role as governors. Any information downloaded from SharePoint onto a personal device should be deleted upon the completion of the task.
- All work-related business should be conducted using the email address the school has provided. Personal email addresses or mobile number should not be used.
- Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.
- Users must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Understand that anything written in an email or document about an identifiable person can be requested via a Subject Access Request and read by that indivdual. Therefore, do not write anything that you would not want that person to read, or that could bring the organisation in disrepute or is counter to the staff code of conduct. This includes the use of emojis, exclamation marks and sarcasm. Consider if the communications you send breach confidentiality or the Data Protection Act, by asking "should the recipient view this information".

- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information, or the data of multiple individuals should be encrypted so that the information is only accessible by the intended recipient. Please ensure that pupils are only named using initials in emails.
- If Users receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. The SBM should be informed immediately so that this can be recorded in the Record of Breaches register under the section "received in error – breach by another organisation"

- If staff send an email in error which contains the personal information of another person, they must inform the SBM immediately and follow our data breach procedure.

USE OF PHONES

- Staff must not give their personal phone numbers to parents or pupils.
- School phones must not be used for personal matters.
- Staff who are provided with the use of a mobile phone as equipment for their role must abide by the same rules for ICT acceptable use.
- The school can record in-coming and out-going phone conversations.
- If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so.
- Mobile phones and personally owned devices may not be used in any way during lesson time unless permission is given by the Head of School. They should be switched off or silent at all times and stored securely out of sight of others. Where phones are used outside of lesson time such as at breaktime they must **not** be used in an area where there are children present. Suitable locations may be the staffroom, PPA room, offices or outside of the school site.
- No images or videos should be taken on mobile phones or personally owned devices. It is not permitted to take photos or videos of children on personal devices. Where photos are taken at staff social events, these should not be published without the express agreement of the people involved.
- Staff are not permitted to use their own mobile phones for contacting children or their families within or outside of the school in a professional capacity unless this is during a lockdown or as a result of self-isolation. This should be agreed with SLT and the and the number is withheld.
- Staff should never send to, or accept from anyone, texts or images that could be viewed as inappropriate or allow children to be 'friends' on social networking sites.
- All users with school emails should ensure their phones are protected with PIN codes in case of loss or theft.
- Staff should never store parents or pupil's telephone numbers on their mobile phone, as this allows the possibility of inappropriate contact. Where staff have friends, who are also parents a clear distinction should be made when in contact. Any matters raised about the school should be treated with care and referred to the appropriate person within school. Staff should take particular care when asked questions as these can be reported back to the school as "Mr/Mrs X said...."
- The taking of personal phone calls during work time should be kept to a reasonable minimum and should generally relate to emergency situations.
- Staff can give the school office number as an emergency contact number for dependents during the working day to minimise the need for checking mobile phones.

SOCIAL MEDIA

Staff should take care to follow the school's guidelines on social media use.

MONITORING OF SCHOOL NETWORK AND USE OF ICT FACILITIES

The school reserves the right to monitor the use of its ICT facilities and network, and access accounts when deemed necessary This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications
- CCTV footage

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

MEMORY STICKS

All staff have a duty of care to ensure all confidential, sensitive and personal information is held securely at all times. The use of non-encrypted memory sticks is prohibited, and staff members found using them may be subject to disciplinary procedures. Any loss of encrypted memory sticks must be reported to the SBM. Confidential, Sensitive and Person Information Data must not be stored or carried on non-encrypted memory stick, laptops or computers, or emailed to personal email accounts.

All members of staff who use memory sticks will be supplied with an encrypted one. This memory stick belongs to the school. However, on leaving staff will be permitted to retain their memory stick on the understanding that they sign a written declaration that any information in any form relating to the school has been deleted. If the memory stick gets lost you must inform the Head of School immediately and will be charged £10.00 for a replacement. If the memory stick is stolen you must contact the Head of School immediately and provide the school with a crime number.

REMOTE ACCESS TO SCHOOL COMPUTERS, PROVIDING REMOTE EDUCATION AND VIRTUAL MEETINGS

Ashford CE Primary School and our IT services, support secure, safe, accessible and available remote access and mobile working through its systems and policies, through the provision of essential technical controls and through raising user awareness and encouraging good working practices. Users with remote access permissions must be aware of procedures and responsible ethical practices.

Remote Access - accessing the school's network from outside of the premises via a different network.
Mobile Working - performing tasks on the network, from connectivity outside of the network (i.e. the creation, storage, processing and transport or transfer of data/ information) as an employee of Ashford CE Primary School.

The primary responsibilities of employees and other users that remote into the school's network are to:

- Know what information they are accessing, using or transferring
- Understand and adhere to contractual, ethical or other requirements attached to the information and pertinent to school policies and procedures.
- Users are responsible for following correct procedures when logging out of the remote session
- Confidential data/information should not be created or stored on privately owned computers. The school strongly encourages the use of the Microsoft Office 365 facilities for working online and storing on the OneDrive or SharePoint facilities.

If users are using their own personal systems or other mobile devices to carry out work for Ashford CE Primary School then the following points should be noted and followed:

- Keep abreast of current security threats and issues for their device type, whether that is related to hardware or software
- Maintain safe web-surfing practice.
- Each device is equipped with up-to-date anti-virus software and other security software such as malware and a configured firewall.
- They perform critical operating System updates as soon as they become available.
- They practice good password controls as appropriate.
- They do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that is not relevant to their role.
- Mobile devices are not left unattended or data that is deemed confidential data is left visible on the screen in public areas.
- If the system has suffered loss of data, corruption of data or any other issues that may impact the network or other systems at Ashford CE Primary it is reported as soon as possible to the SLT and IT support at the School.

The standards and expectations listed above are all to be maintained when organising distance-learning opportunities for children. When using Zoom or any other platform to hold meetings for or about children, the following points should be noted in addition to those above.

- If hosting from home, please be appropriately dressed and ensure, as far as possible, that there are no features in the background that might give clues as to your home address.
- Ensure that there are no items in the background that might be deemed inappropriate or unprofessional (piles of dirty washing, etc.).
- All meetings should be password protected to avoid uninvited participants. Ensure all participants are named before admittance and are not admitted under unrecognised handles such as ‘Ipad7’ or ‘LizardBoy’.
- It is best practice to have two staff members present during a Zoom/online meeting.

Please sign below to say that you have read and understood this information.

Name: **Signature:**

Date: