Date: September 2024
Review: September 2025
Responsibility: Principal/Digital Strategy Leads/
IT Network Manager/Compliance Officer

DAME ALLAN'S SCHOOLS

Whole School Policy on the Acceptable Use of Electronic Devices and Information Technology Systems (External Use)

- **Introduction and scope of this Policy**

1.1 This policy applies to all members of the Dame Allan's Schools' (hereafter the Schools) community, including staff, pupils, parents and visitors. In this policy 'staff' includes governors, teaching and non-teaching staff, visiting music, drama, dance and sports teachers and coaches and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

1.2 The Schools' electronic communication systems and equipment are intended to promote effective communication and working practices, as well as learning tools, for both staff and pupils. They are critical to the way in which the Schools are run.

1.3 This policy outlines the standards the Schools require all users of these systems to follow when using information technology, including equipment situated within the Schools and devices supplied by the Schools to staff and pupils, for use in connection with their employment or education at the Schools.

1.4 This policy deals mainly with the use (and misuse) of computing technology including, but not limited to: software; email; internet connection; social media; telephones (landline, mobile or Google Voice) and voicemail; and all internet enabled devices including Chromebooks, smartphones, tablets, smart watches, and laptops. This policy applies equally to the use of copiers, scanners, CCTV and electronic key fobs and cards.

1.5 All members of the Schools' community are expected to have regard to this policy at all times and any breaches of it will be taken seriously and could result in disciplinary action being taken.

2. Legislative framework

2.1 Use of the Schools' electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the provisions of the Data Protection Act 2018 and the UK General Data Protection Regulation 2018 (GDPR), together with the Employment Practices Code, issued by the Information Commissioner's Office.

2.2 The Schools are also required to comply with the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 and the principles of the European Convention on Human Rights within the Human Rights Act 1998. The Schools are also required to comply with the "Prevent Duty" in the Counter-Terrorism and Security Act 2015.

3. Responsibility for the implementation of this policy

3.1 The Schools' Governing Body has overall responsibility for this policy, but day-to-day responsibility for overseeing and implementing it is delegated to the Principal.

3.2 All members of the Schools' community have a responsibility to operate within the boundaries of the policy, to facilitate its operation by ensuring that they understand the standards of behaviour expected of them and to identify and act upon behaviour, which falls below these standards. Senior Schools' pupils are reminded that a summary of this policy and guidance about e-safety can be found in the information section of their planner. Further guidance information can be found on the policies section of the Schools' website.

3.3 The safe use of electronic communication systems is a child protection and safeguarding requirement. All staff receive training in e-safety issues and the Schools' Designated Safeguarding Leads receive further specific training in safety issues involved in the misuse of the internet and other electronic devices. Further details are set out in the Schools' Safeguarding and Child Protection Policy. All staff are responsible for ensuring and promoting a culture of responsible use of technology, which is consistent with the ethos of the Schools.

4. Online behaviour

4.1 E-safety is addressed through the Schools' curriculum, which ensures that pupils in all year groups are educated about the risks and reasons why they need to behave responsibly online.

4.2 Pupils in Years 7 - 13 are reminded that there is useful guidance given in the information section of their planner about this policy and in the document "Pupil Guidance for Electronic Media".

4.3 All members of the Schools' community should follow the following principles in all of their online activities, including their use of social networking sites:

- All online communications, and any content shared online, must be respectful of others.
- Users should not access, create or share content that is illegal, deceptive, or likely to offend other members of the Schools' community. Examples of such content includes but is not limited to: pornographic content; content that is offensive or obscene; content that promotes violence, discrimination, or extremism; content that raises safeguarding issues; and material that contains confidential information about the Schools or any member of the Schools' community.
- Users should respect the privacy of others. They should not share photos, videos, contact details, or other information about members of the Schools' community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Users should not access or share material which infringes copyright, and should not claim the work of others as their own.
- Users should not use the Schools' local network or the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or to carry out illegal activities.
- Staff should not use their personal email or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.
- Users should remember that whatever is written online remains traceable permanently and is potentially visible to everyone. Posting certain images (for example, self-generated indecent images of a person under the age of 18) on social media sites can easily lead to

someone committing a criminal offence and the evidence trail is extremely easy to follow. The Schools have a duty to report cases of "sexting" to the police and to Children's Social Services and they may result in suspension or exclusion from the Schools, in accordance with the Whole School Behaviour Policy for pupils, and disciplinary measures being taken against members of staff, in accordance with the procedures set out in the Staff Code of Conduct.

- Different social network sites have different age limits for users. Parents are encouraged to make themselves aware of the limits on sites their children are using and monitor their use, wherever possible.
- Privacy settings should always be set at the maximum and checked regularly.
- Passwords should be used wherever possible and these should not be revealed or shared with others. These should be changed regularly.
- When using social networking sites, users should never disclose personal information, neither their own nor that of others. Personal information includes but is not limited to: full names, age, date of birth, phone number, address, and information about the school or other events/venues they attend.
- The Schools' Anti-Bullying Policy sets out the preventative measures and procedures, which will be followed, if the Schools discover cases of bullying, including cyberbullying. Whilst the Schools have no power to control what a pupil puts on their own computers/devices outside of school hours and so have to rely completely on parental supervision, the Schools do, however, have a legal duty to investigate the misuse of social media where it results in bullying or abusive behaviour involving their pupils, and this may result in disciplinary action being taken against a pupil in accordance with our Whole School Behaviour Policy.
- Content online, particularly on social media, which identifies the Schools, can have a damaging effect on the Schools' reputation. The Schools will always take rigorous action to protect their reputation and may take disciplinary measures against any member of staff or pupil, who is found to have created, added to or shared or viewed inappropriately such sites/posts. If a member of staff or pupil becomes aware of potentially damaging online content, they should report it as soon as possible to a member of SMT or the Communications team.
- All members of the Schools' community must report any suspicious online sexual approaches or threatening behaviour, whether from known or unknown sources, to an appropriate person (form teacher, head of year, head of school or member of SMT in the case of pupils and to a member of SMT in the case of staff).
- All users are reminded that text, music and other content on the internet are copyright works and that it is illegal to download or email such content to others unless they are certain that the owner of such work allows them to do so.

5. <u>Using the Schools' IT systems</u>

5.1 Anyone using the Schools' IT systems (including visitors or staff connecting their own devices to the Schools' guest network in the conditions explained in section 6.1) must adhere to the following principles:

- All users are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.
- All users should only gain access to the Schools' IT systems by using their own individual username and password. Users should not share their username or password with anyone else, unless authorised to do so by the IT Support Department.

- When any member of staff leaves the Schools (for whatever reason), they must provide to the IT Support Department the usernames and passwords for all third party sites, apps or services they may have used in the course of their work in the Schools.
- Users should not attempt to gain access to restricted areas of the Schools' network or to any password-protected information, unless authorised to do so; neither should they attempt to alter the Schools' IT systems, nor circumvent the content filters or other security measures installed on them.
- The use of external storage devices, including flash drives and USB memory sticks on Schools' equipment is permitted but limited to copying data from devices. In specific circumstances, and only by authorisation of the IT Support Department, this restriction may be lifted to enable writing of data to specific devices.
- Users should not attempt to install software on the Schools' IT systems. Any software used on the Schools' IT systems must be checked by the IT Support Department prior to its purchase and/or downloading. The use by any member of staff of any software, which has not been previously checked and/or authorised by the IT Support Department, may result in disciplinary action, due to the risk of viruses entering the Schools' systems, which leave them open to a cyber-attack and which may cause us to be in breach of our obligations under data protection legislation.
- Staff must not use a website, app and/or Chrome extension or add-on, with pupils, which requires the setting up and use of an online account, without obtaining permission from the IT Support Department and the Data Protection Coordinator. A Google form is available on the Staff Portal for making such requests.
- Users should not use the Schools' IT systems in a way that breaches the principles of online behaviour set out above in paragraph 4.
- Users are reminded that the Schools monitor use of their IT systems, and that the Schools can view content accessed or sent via its systems.

5.2 Any IT property, including cabling, belonging to the Schools should be treated with respect and care, and used only in accordance with any training and policies provided. Any faults or breakages should be reported without delay to the IT Support Department.

5.3 All staff who have been issued with a Chromebook, or any other device, are reminded that these remain the property of the Schools. Pupil-issued Chromebooks remain the property of the Schools until final payment for it has been made; however, pupils are reminded that all use of their device is subject to the provisions of this policy including when the device is used out of school in their own homes. All users should ensure that their device is kept safe and secure at all times, especially when travelling, and should have regard to the provisions of the Schools' Data Protection Policy and Privacy Notices and ensure that any personal data is protected in the event that the device is lost or stolen.

5.4 The provision of Schools' email accounts, Wi-Fi and internet access is for official Schools' business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit, as far as possible, any personal use of these accounts. Users are reminded of the Schools' right to monitor and access web history and email use.

5.5 All official business relating to the Schools must be conducted on the Schools' systems, and it is not permissible to use personal email accounts or messaging services to conduct Schools'

business. Any use of personal devices for Schools' purposes, and any removal of personal data or confidential information from the Schools' systems – by any means including email, printing, file transfer, cloud or external storage device – must be approved in advance by the IT Support Department. In some instances the Senior Management Team may become involved in order to assess the reasons for removal of data and oversee the process.

5.6 Where permission is given for use of personal devices for Schools' business, these must be subject to appropriate safeguards in line with the Schools' policies, including the use of passwords, two-factor authentication and encryption. You will be required to install a Google Device policy "app" if you add your school Google account to a personal device, this ensures your device is compliant with the Schools' policies and helps to keep a separation between personal files/apps and School files/apps.

5.7 Members of staff are referred to the relevant provisions of the Staff Code of Conduct, in particular:

- paragraph 12 - Communication with Children and Young People (including the use of technology);
- paragraph 24 - Photographs and videos;
- paragraph 25 - Access to Inappropriate Images and internet usage;
- paragraph 26 - Use of the Schools' social media accounts;
- paragraph 27 - Guidance on e-safety;
- paragraph 28 - Guidance on the use of technology for online/virtual teaching.

5.8 Whilst the Schools permit staff and pupils the incidental use of their internet and email systems to send personal email, browse the web and make personal telephone calls, this is a privilege and not a right and should not be abused or overused. Use of the Schools' systems in this way may be monitored, as set out in paragraph 9 below.

5.9 The Schools reserve the right to withdraw this permission or amend the scope of the permission, which is as follows:

- Use must be minimal and take place substantially out of normal school hours;
- Personal emails must be labelled "personal" in the subject header;
- Use must not interfere with the Schools' commitments;
- Use must not commit the Schools to any costs; and
- Use must not be in breach of any of the Schools' policies.

5.10 Visitors to the Schools, who require access to technology, may be provided with an electronic device or computer. Alternatively, they may be provided with access to the guest wifi network to use with their own devices. They will be able to use the Schools' systems using a guest username and password and no access to data or shared storage drives would be provided without prior approval by the IT support team and the Principal.

6. <u>Use of Chromebooks and own devices</u>

6.1 All pupils and some staff have been issued with Chromebooks by the Schools for use in connection with their education and employment. Accounts other than the one provided by

the Schools should not be added to the Chromebook. Pupils and staff may bring to the Schools their own electronic devices, such as laptops, tablets, smartphones and other devices but these devices may not be connected to the school network, other than in exceptional circumstances authorised by the Senior Management Team and subject to the security measures outlined in 6.7.

6.2 All of the above devices must be used in accordance with this policy. The Schools reserve the right to refuse to allow access to particular devices or software, where they consider that there are security or other risks to the Schools' systems and/or infrastructure. All users are expected to play their part in maintaining the security of the data they handle. Any security incident involving a pupil or member of staff using their own device whilst at the Schools will be taken very seriously and will be investigated and reviewed by the IT Support Department, who will advise the Principal on the most appropriate course of action. Depending on the seriousness, this may result in sanctions being put in place and external agencies being involved.

6.3 Pupils should not use their own devices in school at all, except in exceptional circumstances (for example, to contact a parent), and only with the explicit permission of a member of staff and under close adult supervision. The exception to this is Year 12 or 13 pupils, detailed further in paragraph 6.6. Any pictures/audio/video taken during the course of a lesson may only be used for the purpose for which it is taken (i.e. for school work) and it must not be uploaded online, shared or broadcast unless the teacher has given specific permission. They must be stored on the Schools' systems and deleted from a pupil's own device. When they are no longer needed, they should be deleted from the device. In no circumstances will pupils' personal devices be connected to the Schools' WiFi network.

6.4 During break and lunch times and prior to morning registration, pupils in Years 7 -11 may use their school-issued Chromebook in the catch up room, the library and form rooms without supervision, subject to these conditions:

- It should be used predominantly for academic purposes
- Any games played on the device must be certified at the correct level for the user.
- Social networking sites and online messaging systems must not be accessed.
- Chromebooks must never be used in the corridors.
- Chromebooks may only be used in the dining hall during after school care.

6.5 Junior School pupils are not permitted to use their own devices at any time whilst on School premises. Whilst the Schools understand the convenience of using mobile phones (for example, children going home by bus) they and other electronic devices must be handed in to the class teacher for safe keeping at the beginning of the day and collected after the final lesson. Phones and other devices should be clearly labelled. Under no circumstances should a mobile phone or other device be left in a bag, or in a pocket, whether switched on or off. If a pupil unwittingly forgets to hand in a mobile phone and it rings in a lesson then the phone will be confiscated. It will be returned to the pupil at the end of the day with a proviso that should this happen again then the pupil will be sent to the Head or Deputy Head of the Junior School. At this point the pupil will be warned that (in consultation with his / her parents) he or she will not be allowed to bring in the phone until a set date. If a mobile phone or other device is used at any time during the school day for any purpose, then the phone or other

device will be confiscated and the pupil sent to the Head or Deputy Head of the Junior School. A letter will be sent home informing parents of the incident.

6.6 Other than in lessons or during study periods, pupils in Years 12 and 13 may only use their own devices or school-issued Chromebooks to make phone calls, access the internet appropriately or listen to music within the group work area and garden of the Queen's Building. They are not to be used anywhere else on the Schools' sites.

6.7 Where personal devices are used under the provisions of 6.1, devices **must** comply with following security requirements:

- the device must have the latest updates to the operating system
- all software on the device must be licenced and up to date with patches
- If available, the device needs to have an antivirus and firewall installed, enabled and up to date
- the device should have an unlock credential such as biometric, password or PIN
    - Ideally this should not allow more than 10 guesses in 5 minutes and locks the device after no more than 10 unsuccessful attempts
    - PIN length if used should be no less than 6 characters

6.8 No member of staff working in the EYFS department may have their own camera adapted mobile phone, their own camera or recording equipment in their possession whilst working with children in the department. Due to the presence of EYFS children, members of staff working at the Junior School must not have their own mobile phone, their own camera or recording equipment in their possession during the School day. Such devices must be locked in classroom desk drawers or in the staff room. At both the Junior and Senior Schools members of staff should not use their own mobile phones, cameras and recording devices in the presence of pupils, except in an emergency. Where staff do take photographs and videos of pupils (for example, for Class Dojo and Tapestry at the Junior School, for internal displays or for use on the Schools' social media feeds), they MUST only use a device issued by the Schools. They must NEVER use their own device for taking images of pupils.

6.9 It is the responsibility of each pupil and member of staff to keep their Chromebook and their own devices safe whilst at the Schools and the Schools cannot be held responsible for any loss or damage to any such devices. If a Chromebook is damaged or defaced deliberately, through abuse or neglect, it must be repaired or replaced. Whilst some repairs may be covered by the 3 year warranty (commencing from the time it was purchased by the Schools) or accidental damage cover (such cover allows 1 claim per year only), if the repair is not covered by the terms of the warranty/accidental damage cover and/or the warranty/accidental damage has expired, a charge will be made for those repairs. If the device is out of warranty you will be given the option to get the device repaired yourself or to buy a new replacement. The Schools recommend that each device is insured, not left unattended and that pupils store their own devices in a locked locker when not in use. The following are not permitted:

- writing on, engraving, or in any other way defacing or marking the Chromebook;
- removing or modifying any part of the Chromebook;
- attempting to disassemble the Chromebook;

- attempting to replace any part of the Chromebook.

6.10 In the event of loss or theft of a device, including a school-issued Chromebook, the user must change their password to all of the Schools' services accessed from that device. In addition, the loss or theft of the device must be reported promptly to the IT Support Department in order for access to the Schools' system by that user or device to be revoked. It must also be reported to the Schools' Data Protection Coordinator, so that any loss of personal data, which may result in a breach of GDPR, can be investigated and, if deemed sufficiently serious, reported to the ICO.

6.10 School-issued Chromebooks are allocated an IP address. Users must not attempt to edit, adjust, mask or share the IP address their Chromebook has been provided with. In the event that anyone is found to have done so, their access to the Schools' systems may be revoked and disciplinary action taken.

6.11 School-issued Chromebooks have stickers attached in order to identify it and who it belongs to. These stickers should not be removed or obscured under any circumstances. If this sticker has come off or has been damaged, the IT Technicians and/or a teacher or Form Tutor should be informed as soon as possible.

6.12 Pupils are responsible for ensuring that they bring their Chromebook to school every day and that it is charged and ready to be used by the start of the School day as the Schools are unable to provide electrical outlets for pupils to use for charging devices. Any pupil found to be using an electrical outlet for charging a device will have that device removed for the remainder of the school day or sanctioned appropriately. If chargers are lost or damaged, it is the user's responsibility to replace this. Suggested replacements can be found at https://chromebook.dameallans.co.uk/replacment-parts

6.13 Users may face disciplinary action if they attempt to or use any device which creates its own wireless hotspot or connects to a hotspot.

6.14 The Schools allow access to the Google Workspace Marketplace and Chrome Web Store to enable pupils to install apps that are required for their learning, provided they have been approved by the IT Support Team. No user should download an app using the Schools' systems, which is for personal use. Access to a wide range of online software that is used through the Google Chrome web browser is provided via the school Google account. This software may be used as long as, by doing so, this Acceptable Use Policy is not contravened.

6.15 Users should not attempt to change any Chromebook settings, other than those provided within the user account (e.g. font size, keyboard settings, and screen brightness).

6.16 Parents will be asked to purchase a new Chromebook every 5 years. However, as newer versions of Chromebooks become available more frequently than every 5 years, pupils and their parents will have the opportunity to purchase the latest model at the start of each academic year. When a pupil leaves the Schools or purchases a new Chromebook, their Chromebook must be disposed of appropriately as follows:

- a Chromebook can be returned to the Schools, where it will be recycled in an appropriate manner; or
- the pupil can retain their Chromebook and sign a disclaimer agreeing to dispose of it in an appropriate manner in accordance with the Waste Electrical and Electronic Equipment recycling Regulations (WEEE) at https://chromebook.dameallans.co.uk/unregister.

6.17 Chromebooks use Google Drive cloud storage to store all documents, meaning that they can be accessed from any computer or device which has internet access. The Schools' Google account should only be used for activities and documents that are directly related to the Schools. Chromebooks or any of the Google services provided by the Schools should not be used to store, share or transmit personal documents, files or information that is not directly related to the Schools.

6.18 The Schools take no responsibility for supporting users' own devices. Any support is provided at the discretion of the IT Support Team and will be secondary to their primary task of maintaining the Schools' core systems.

7. Photographs and videos

7.1 All members of the Schools' community are referred to the provisions of the Schools' Taking, Storing and Using Images of Children Policy. Members of staff must also follow the provisions of the Staff Code of Conduct, in particular paragraph 24 (Photography and Videos).

7.2 Use by pupils of the camera and/or microphone function on a Chromebook (including the use of Screencastify), phone or other image/video/audio recording device without permission from a member of staff is a disciplinary offence which attracts sanctions outlined in the Whole School behaviour policy, up to and including exclusion from school. This includes anywhere in the Schools, not just the classroom. Recording audio, video or photographs using a Chromebook at home should only be done for the purposes of schoolwork under instruction by a teacher, and with your parent's permission. This will be treated as such a serious offence because of the possibility of bullying as a result of such images being manipulated, for example by the possible placement of the images on the Internet, or by images being sent to other people's phones. Such actions constitute a serious breach of an individual's human rights. Photographing and recording any member of the School's staff (teaching or support) without their expressed consent is an extremely serious offence and will incur a serious sanction. Even authorised images of staff may not be uploaded or copied to other devices or sites and must be destroyed/deleted as soon as possible after the authorised use.

8. Systems and data security

8.1 All members of the Schools are reminded that the Schools' IT systems must only be used in accordance with this policy and they must have regard to the Schools' Data Protection Policy (in particular paragraph 14) and their obligations under GDPR to keep all personal data secure.

8.2 No user of the Schools' IT systems should delete, destroy or modify any existing systems, programmes, information or data, which could have the effect of harming the Schools' operation or exposing it to risk, including that of cyberattack.

8.3 Users should not attempt to gain unauthorised access to anyone else's Chromebook or computer or to confidential information to which they do not have access rights. Users should not use a Chromebook, computer or service signed in using another user's account, even if the account owner is aware of it.

8.4 Whilst the Schools' systems monitor all emails for viruses, all users should exercise caution when opening emails from unknown sources. Where an email appears to be suspicious, it should not be opened and the IT Support Department should be informed immediately. The Schools reserve the right not to transmit any email and to block access to attachments to emails for the purpose of effective use of the IT system and for compliance with this policy.

8.5 Passwords protect the School's network and computer system and are everyone's responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised.

8.6 Passwords protect the School's network and computer system and are everyone's responsibility. Requirements for the complexity of passwords are published internally.

8.7 The Schools deploy website/email filtering in order to safeguard pupils from potentially harmful and inappropriate online material.

It is important to recognise that no filtering systems can be 100% effective and these need to be supported with good teaching and learning practice and effective supervision. As per the UK Safer Internet Centre guidance, illegal online content and inappropriate content (and web searches) are blocked, including (but not limited to):

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of the protected characteristics listed in the Equality Act 2010
- Drugs/Substance abuse: displays or promotes the illegal use of drugs or substances
- Extremism: promotes terrorism and terrorist ideologies, violence or intolerance
- Malware/Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- Pornography: displays sexual acts or explicit images
- Piracy and copyright theft: includes illegal provision of copyrighted material
- Self Harm: promotes or displays deliberate self harm (including suicide and eating disorders)
- Violence: Displays or promotes the use of physical force intended to hurt or kill

The Schools may also block categories/websites that prove distracting or unsuitable. (e.g. games)

Categories which are blocked are reviewed annually by the ICT Steering Committee.
Day-to-day responsibility for checking/changing a website's category falls to the ICT Support department with approval by SMT if necessary.

Monitoring is provided by automated alerts, daily reports, weekly reports and ad-hoc reports when necessary.

9. **Emails**

9.1 Whilst the Schools recognise the email is a vital means of communication, all members of the Schools' community are reminded that it should be used with great care and discipline. Emails should be written as professionally as a letter and users should always consider whether email is the appropriate medium for a particular communication.

9.2 All users are reminded of the following:

- Do not send or forward private emails, which you would not want a third party to read, including jokes or gossip.
- Do not contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have any need to receive them. Equally do not create or forward "chain letters" or other "pyramid" schemes of any kind.
- Do not agree to terms, enter into contractual obligations or make representations by email unless appropriate authority has been obtained.
- Do not send confidential messages via email or the internet, or by other means of external communication, which are known not to be secure.
- Do not send emails to large numbers of recipients unless absolutely necessary, especially if they contain sensitive personal data relating to individuals. If this cannot be avoided, remember to "blind copy" (bcc) email addresses, so as to avoid recipients seeing the email addresses of others or use the groups set up on iSAMS.
- Emails may need to be disclosed to a person who makes a Subject Access Request to the Schools for the disclosure of their personal data. Emails should not contain personal opinions about other members of the Schools' community and must use appropriate language at all times.

9.3 Any user who receives an email which has been wrongly delivered, should notify the sender and delete the email immediately. If the email contains confidential information or inappropriate material, it should not be disclosed or used in any way. The user must also inform the Schools' Data Protection Co-ordinator about the receipt of the email, so that steps can be taken to investigate whether the provisions of the GDPR have been breached and whether this needs to be reported to the ICO.

9.4 All staff are expected to check their school emails at least once per day and they should respond to emails from parents and pupils within 2 working days and to other members of staff as soon as possible, but within 2 working days. Parents and pupils are reminded that members of staff will not be expected to read or reply to emails sent or received out of school hours.

9.5 The same principles, set out in paragraph 4 of this Policy, apply to the content of emails. Emails, which contain abusive, obscene, discriminatory, racist, harassing, derogatory, sexist, homophobic or defamatory content, should never be sent. If they are received, they should not be forwarded and should be reported immediately to the IT Support Department or an appropriate member of staff. The sending of emails, which contain anything of this nature, may result in disciplinary action being taken.

10. Monitoring and access

10.1 All members of the Schools' community should be aware that the Schools' systems provide the capability to monitor telephone, email, voicemail, internet usage (including through the Schools' Wi-Fi) and other communications traffic. Use of the Schools' systems – including the computer systems, and any personal use of them – is continually monitored by the IT Support Department in order to enable the Schools to function effectively and to meet their legal obligations. Monitoring will only be carried out to the extent permitted or required by law and as necessary and justifiable for the Schools' purposes.

10.2 CCTV is used to monitor parts of the Schools' buildings. Use and storage of this data is covered by the Schools' CCTV policy.

10.3 The Schools reserve the right to retrieve the contents of messages or check searches which have been made on the internet for the following purposes (which are non-exhaustive):

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this and other Schools' policies.
- To find lost messages or retrieve those lost due to computer failure.
- To assist in the investigation of wrongful acts.
- To comply with any legal obligation.

10.4 Content on user-owned devices is not logged, other than when users are signed in to their Schools' Google Account, where content such as files in Google Drive can be monitored. The Schools' reserve the right to monitor any traffic over their systems in order to prevent threats to their infrastructure and data and to comply with the Schools' safeguarding policy.

10.5 The Schools may require access to a pupil's personal device when investigating breaches of the Schools' policies, including but not limited to cyber bullying, hacking of Schools' systems, virus attacks and inappropriate use of the Schools' systems. This process will only be carried out by the IT Support Department on the express instruction of the Principal and every effort will be made to ensure that the Schools do not access any private information contained on that device.

11. Retention of digital data

11.1 The Schools' Retention of Records Policy sets out the Schools' policy on the retention of records, including digital data. It follows the principle set out in data protection legislation that data should only be retained for as long as it is necessary.

11.2 At the end of each term, members of staff are requested to review all of their emails sent and received on their school account and to delete or archive emails, as appropriate. When a member of staff leaves the employment of the Schools, their email account is deleted within one year of them leaving, save that the email accounts of any member of the Schools' senior management team, who leaves the Schools' employment, may be kept open for a period of up to 2 years, before emails therein are archived.

11.3 The emails of pupils, who leave the Schools at the end of Year 13, will be deleted 3 months after their departure date, which is deemed to be 31st August. If access is required for longer, users must contact the IT Support Department in writing prior to their email accounts being disabled. The email accounts of all other pupils who leave the schools will be deleted 6 months after their departure date.

11.4 The Schools will endeavour to ensure that no important information is ever lost as a result of an email being deleted. Important information that is necessary to be kept should be held in the relevant HR or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information (or indeed any personal information that they wish to keep, in line with school policy on personal use) is retained in the correct place or, where applicable, provided to the right colleague.

11.5 If a user considers that reasons exist for the policy not to apply, or needs assistance in how to retain and appropriately archive data, they should contact the IT Network Manager.

12. **Breach reporting**

12. 1 The law requires the Schools to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This will include almost any loss of, or compromise to, personal data held by the Schools regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the Schools' systems, for example, through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email; and
- unsecure disposal.

12.2 The Schools must generally report personal data breaches to the Information Commissioner's Office (ICO) without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the Schools must keep a record of any personal data breaches, regardless of whether we need to notify the ICO. If a member of staff or a pupil becomes aware of a suspected breach, they must notify the Schools' Data Protection Coordinator in accordance with the procedures set out in the Schools' Data Protection Policy and, for members of staff, the Staff Code of Conduct.

12.3 Data breaches will happen to all organisations, but the Schools must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The Schools' primary interest and responsibility are in protecting potential victims and having visibility of how effective their policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach to the Data Protection Coordinator will be a disciplinary offence.

13. Breaches of this policy

13.1 Any breach of this policy may be dealt with as a disciplinary matter using the Schools' disciplinary procedures for pupils (as set out in the Whole School Behaviour Policy) and staff (as set out in the Staff Code of Conduct and the Disciplinary Procedure). In addition, a deliberate breach may result in the Schools restricting that person's access to the Schools' IT systems.

13.2 If any member of the Schools' community becomes aware of a breach of this policy or has any concerns that a member of the Schools' community is being harassed or harmed online, they should report it to the Schools' Digital Strategy Leads, either at the Senior or Junior Schools. Any such reports will be treated in confidence. Alternatively, any child protection and/or safeguarding concerns should be reported to a DSL, in accordance with the Safeguarding and Child Protection Policy.

14. Compliance with related Schools' policies

This policy should be read in conjunction with the following:

- Data Protection Policy
- The Schools' Privacy Notices for parents, pupils, staff, governors and suppliers, contractors and volunteers;
- Safeguarding and Child Protection Policy
- Staff Handbook;
- Staff Code of Conduct;
- Whole School Behaviour Policy;
- Anti-bullying Policy;
- Whistleblowing Policy;
- Taking, Storing and Using Images of Children Policy;
- Retention of Records Policy;
- Pupil and Parent Social Network Guidance;
- Pupil Guidance for Electronic Media;
- Department for Education Guidance on Cyberbullying - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf