Online Safety
and
Acceptable Use Policies

for the whole School including EYFS

Policy revised by	DFB
Last SLT Review	November 2021
SLT Review Period	2 years
Next SLT Review Due	November 2023
Governor Review Period	2 years
Governing Committee	IT Committee
Next Review Due	November 2023

School Mission and Values

Beechwood Park's Mission is to be the first-choice preparatory School for parents considering an independent education recognised for its outstanding quality of educational experience and care.

To fulfil this ambition, with the support of parents, the School:

• **Nurtures** and promotes the happiness, health, safety and emotional well-being of every child, developing in them confidence and independence
• **Engages** the intellectual, physical and spiritual potential of every child across a broad range of academic, extra-curricular and pastoral activities and experiences
• **Inspires** children, inculcating transferable, lifelong skills and values by which to achieve personally, and contribute influentially to society
• **Enables** inspirational and reflective teachers to provide every pupil with outstanding teaching, delivering the highest levels of educational pace, variety and challenge.

The Schools 16 core **Values** underpin our *Mission*.

Introduction

Beechwood (hereafter, sometimes 'the School') staff, including employees, contractors, sole traders and volunteers, are role models and are in a unique position of influence over young people. They therefore, adhere to behaviours and values that set a good example to all the pupils within the School.
The School teaches pupils the skills required to access the many technologies necessary for life-long learning.
Digital learning includes instruction in both web-based and mobile learning and recognises the constant and fast-paced evolution of digital learning.
The School understands its responsibility to educate our pupils on **Online Safety** issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and out of the classroom.

Government Guidance

This policy should be read in conjunction with the non-statutory DfE guidance document: Teaching online safety in School (June 2019) and the DfE's Education for a Connected World (June 2020). These documents inform the School's curriculum teaching regarding Online Safety.

Associated Policies

Please read this policy and the following policies and documents:

- *BPS Anti-Bullying Policy*
- *BPS Child Protection Policy*
- *BPS Pupil Conduct Policy*
- *BPS Data Protection, Record Keeping and Disposal of Records Policy*
- *BPS Health and Safety Policy and Handbook*
- *BPS Learning Support Policy*
- *BPS Safeguarding Cause for Concern Record (C4C)*
- *BPS School Trips and Visits Policy*
- *BPS Staff Behaviour Policy*
- *BPS Staff Recruitment Policy*
- *BPS Staff Whistleblowing Policy*
- *BPS Taking, Storing and Using Images of Children Policy*
- *BPS Visiting Speaker Policy*
- *BPS Covid-19 Risk Assessment*
- *DfE Sexual Harassment and Sexual Violence Advice*
- *Keeping Children Safe in Education September 2021*
- *Working Together to Safeguard Children 2018 including Annex A*
- *Data Protection Act 2018 and General Data Protection Regulation (GDPR)*
- *ISI Safeguarding for Remote Teaching*
- *Sharing nudes and semi-nudes: how to respond to an incident*

Roles and Responsibilities
This policy for staff, (including employees, contractors, sole traders and volunteers), governors, visitors and pupils, protects the interests and **Online Safety** of the whole School community.

Governors
The *Full Board of Governors* has overall responsibility to oversee the highest levels of Online Safety.

Committees
The *Full Board of Governors* delegates this responsibility to both the *IT Committee* and the *Pastoral Care and Welfare Committee*, both of which monitor the effective implementation of the School's *Online Safety Policy*.

Leadership
The *IT Committee* and *Pastoral Care and Welfare Committee* through the *Deputy Head (Academic)* and *Deputy Head (Pastoral)* delegate the technical and pastoral management of Online Safety to the *Director of Digital Learning*.

Management
The *Director of Digital Learning*:

- Writes punctual reports for both committees, updating them on Online Safety developments and ensures that they remain up to date with technological change;
- Has sole responsibility for ensuring that all staff, pupils, parents and governors have access to and understand this key School policy;
- Keeps this policy up to date and compliant with law and best practice; Ensures that all staff, pupils, parents and governors understand their responsibility with regards to **Online Safety**;
- Keeps abreast of current issues and guidance through organisations such as *CEOP (Child Exploitation and Online Protection)*, *Childnet*, the *Hertfordshire Safeguarding Children Partnership, UK Council for Child Internet Safety, Global Kids Online, Digital Futures Commission, Naace, and Better Internet for Kids;*
- Ensures that organisations letting from the School follow all aspects of the *BPS Online Safety Policy* and *Acceptable Use Agreements*;
- Delivers information and training on *Online Safety (Channel and Prevent)* to staff in staff meetings, emails, e-Learning and memos;
- Runs a daily *Safeguarding Monitoring Report* which monitors all website traffic, alerting the *DSL* without delay of any concerns;
- Ensures that all new staff sign the *BPS Acceptable Usage Policy* as part of their induction process, recording AUPs with the *HR Department;*
- Trains all staff in their individual responsibilities relating to the safeguarding of children in **Online Safety** and ensures that they know what to do in the event of misuse of technology by any member of the School community, including cyberbullying;
- Provides resources to all staff to incorporate **Online Safety** activities and awareness within their teaching, PSHEE and assemblies;
- Produces regular letters, keeping parents and their children, governors and staff informed of **Online Safety** issues and advice;
- Advises staff, governors, parents and pupils how to manage screen time safely;
- Advises staff, governors, parents and pupils about certification of films and electronic games and posts appropriate **Online Safety** messages in all networked rooms;
- Finds opportunities to present **Online Safety** messages through email, through assemblies, newsletters and PSHEE;
- Embeds **Online Safety** as a core topic at the start of every year's Digital Learning lessons, finding opportunities when relevant, to discuss **Online Safety** in Digital Learning lessons as the year progresses;
- Informs staff, governors, parents and pupils that the School monitors network and internet use;
- Displays **Online Safety** posters prominently, especially in the IT Rooms;
- Produces and distributes **Online Safety** (and Prevent) posters to be displayed in ancillary areas including all staffrooms, boarding areas, Maintenance and Catering areas and Music Department; Informs the *Designated Safeguarding Lead* without delay, of any safeguarding concerns;

- Records that all pupils in Years 3 an above have read and signed the pupil AUP statement annually; Assists the *Deputy Head (Academic)* and the *Deputy Head (Pastoral)* with all **Online Safety** investigations.

The *IT Manager:*

- Ensures that the School's technological infrastructure is secure and, so far as is possible, is not open to malicious use or attack;
- Monitors technology uses and practices across the School;
- Assesses whether any improvements can be made to ensure **online safety**.
- Ensures that the School has an effective filtering policy in place and that is applied and updated on a regular basis.
- Ensures that that the use of the School's technology is regularly monitored and backed-up and that any misuse or attempted misuse can be identified by the *Director of Digital Learning*.
- Ensures that monitoring software and systems are kept up to date to allow the tracking the use of email and the internet over the School's network and maintain logs of such usage.

Online Safety in the Curriculum
Online Safety educational content focuses on three key areas, as highlighted in *Keeping Children Safe in Education September 2021:*

Content: Being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;

Contact: Being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and

Conduct: Personal online behaviour that increases the likelihood of, or causes, harm; e.g. making, sending and receiving explicit images, or online bullying.

The *Director of Digital Learning* ensures that all pupils understand:

- The positive and negative impacts of technologies in and out of School or during Remote Learning, on them, their colleagues, parents and beyond and the consequences of negative online behaviour.
- How to implement copyright etiquette and respect other people's information, images and the use of Creative Commons licencing.
- The definition of cyberbullying and the impact of online bullying and how to seek help if they are affected by these issues. How to treat each other's online identities with respect.
- How to keep control of their digital footprint.
- How to shape a positive digital identity for themselves.
- To recognise the difference between their digital rights and their digital responsibilities.
- How to recognise suspicious, bullying or extremist behaviour.
- How to seek advice or help if they experience problems when using the internet and related technologies.
- How to evaluate materials and learn good searching skills and to be critically aware of the content they access online and guided to validate accuracy of information.
- How to build practices to help them to adjust their behaviours so as to reduce risks and build resilience.

As detailed in the *BPS Anti-Bullying Policy* and *BPS Staff Behaviour Policy*, staff are reminded that cyberbullying is as unacceptable when carried out by staff members as it is when carried out by pupils.

Surveys

Michaelmas Term

The *Director of Digital Learning* conducts an annual **Online Safety** survey of all pupils, presenting their findings and clear recommendations to both the *IT Committee* and the *Pastoral Care and Welfare Committee* at their committee meetings in the *Lent Term*. They add these recommendations to the ***Online Safety*** *Development Plan,* published on *SharePoint*.

Lent Term

The *Director of Digital Learning* conducts an annual **Online Safety** survey of all staff in the Lent Term, presenting their findings and clear recommendations to both the *IT Committee* and the *Pastoral Care and Welfare Committee* at their committee meetings in the Summer Term. They add these recommendations to the ***Online Safety*** *Development Plan*, published on *SharePoint*.

Summer Term

The *Director of Digital Learning* conducts an annual **Online Safety** survey of all staff in the Summer Term, presenting their findings and clear recommendations to both the *IT Committee* and the *Pastoral Care and Welfare Committee* at their committee meetings in the Michaelmas Term. They add these recommendations to the ***Online Safety*** *Development Plan*, published on *SharePoint*.

Password Security

The *Director of Digital Learning* ensures that all pupils from Year 3 and all staff have individual log-ins and storage folders on the School network.

The *Director of Digital Learning* reminds staff and pupils regularly of the need for password security for the internet and ensures all pupils from Year 5 onwards have passwords.

Data Security

Please refer to *BPS Data Protection, Record Keeping and Disposal of Records Policy*. The *Director of Digital Learning* reports on data security matters termly at every *IT Committee* and the *Pastoral Care and Welfare Committee*.

Monitoring

The *Director of Digital Learning* agrees the scope of any monitoring of staff communication in writing with both the Headmaster and Bursar. They will consider the following legislation:

- *Data Protection Act 2018 and General Data Protection Regulation (GDPR)*
- *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000,*
- *Regulation of Investigatory Powers Act 2000,*
- *Human Rights Act 1998 and*
- *Keeping Children Safe in Education September 2021.*

Managing the Internet

The *Director of Digital Learning* reports on all breaches of the AUP without delay to the Headmaster and Bursar. Where there is a safeguarding concern, the *Director of Digital Learning* reports the incident without delay to the *Designated Safeguarding Lead* in accordance with safeguarding policy.

Filters

The *School Firewall (WatchGuard)* and *Web Filter (Smoothwall)* control access to the School internet. The filter excludes by category and key words. Use of the web filter considers the age range of pupils, number of pupils, how often they access the IT systems and the proportionality of costs vs. risks.

The *Director of Digital Learning*:

- Recognises that no filtering system can be 100% effective and that effective online learning practice and supervision support this.
- Ensures that all staff are aware that they need to preview sites, software and apps before their

use in School or before recommending them to pupils.
- Ensures that all staff consult with him with details of the site/service before using any online service that requires user accounts to be created or the sharing of any personal data.
- If teaching staff set internet research for homework, they suggest specific sites ensuring that they have previously checked them.

The *IT Manager* installs anti-virus protection (*Sophos*) and keeps it up-to-date on all School machines, ensuring that the Headmaster knows of any lapse in protection.

Copyright
The *Director of Digital Learning* reminds staff frequently of the importance of adhering to copyright legislation. The *Director of Digital Learning* teaches pupils about copyright and Creative Commons licensing in Computing lessons.

Managing other Web technologies
The *Director of Digital Learning* teaches pupils to:
- Avoid giving out personal details on such sites which may identify them or where they are (full name, address, date of birth, mobile / home phone numbers, photographs, School details, messaging / email address, specific hobbies / interests);
- Avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online;
- Use avatars as visual representations of their online personae;
- Set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals and to Google Search results;
- Be wary of publishing specific and detailed private thoughts online;
- Be aware of the role that web browsers and search engines play in tracking their online behaviour;
- Be discerning in their choices of online tools;
- Learn how to triangulate the sources of information they discover online in order to verify its veracity;
- Avoid plagiarising content found on the Internet;
- Recognise that in school a filter protects them from accessing unsuitable content but at home they need to be more vigilant;
- Consider carefully anything that is posted online whether through messaging, social media or by other means, only posting messages that they would be happy for a teacher, parents or guardian to see; Avoid viewing, retrieving, downloading or sharing of any offensive material;
- Never give their personal email address to any website requiring a sign up in school;
- Never use a personal email address when contacting any adult member of the school community;
- Not to communicate with staff using social networking sites or other internet web-based communication channels;
- Report any incidents of bullying to the School or incidents whereby pupils have been targeted or influenced to participate in radicalism or extremism to their *Form Teacher, Director of Digital Learning* or *Deputy Head (Pastoral)* in line with the *BPS Anti-Bullying Policy*;
- Understand that any device that can or has the potential to be connected to a cellular network, or can seamlessly connect to another device using Bluetooth or similar technology (including smartphones), may not be used by a student in School without specific permission being given *(until such time as a BYOD policy is implemented)*.

Personal Mobile devices
Please refer to the *BPS Staff Behaviour Policy* and *BPS Child Protection Policy*. The School is not responsible for the loss, damage or theft of any personal mobile device. Users bringing personal devices into School must ensure that there is no inappropriate or illegal content on the device. A Guest Wi-Fi code is available for adult guests from Reception.

Staff must never use their own mobile devices whilst working with children, except in an emergency. Staff may use personal mobile devices during breaks and only in locations where they cannot be seen

or overheard by pupils, parents or visitors.

Under no circumstances may staff use personal mobile phones in, or in the vicinity of, *Woodlands*, *Reception*, or in the *Junior Department*.

Email Communications
The School provides all staff with their own email account to use for all School business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the revelation of risk of personal profile information.

Staff check emails carefully before sending them, ensuring a high level of accuracy. Staff check email communication intended for a group of parents with their line manager and/or with the HM as appropriate.

Teaching staff ensure that pupils only use School-approved email accounts on the School system under direct teacher supervision and for educational purposes.

E-mail users use appropriate language and abide by GDPR Policies, not revealing personal details about themselves and virus checking attachments.

The *Director of Digital Learning* reminds pupils to tell a teacher without delay if they receive an offensive email or cyberbullying e-mail.

The use of 'Reply All' is to be used judiciously, and chosen with care.

In line with good 'netiquette', Staff must avoid adding individuals who were not in the original circulation later in an email chain

In accordance with GDPR regulations, a member of staff's personal email address must not be used for school-related business without that member of staff's permission.

In accordance with GDPR regulations, if personal email addresses of members of staff are to be used in emails circulated for school-related purposes, then such addresses must be included as BCC.

Staff must use distribution lists judiciously, in particular 'All Staff' as in this circumstance, the email will go to all Beechwood employees.

As explained in more detail in the BPS Staff Behaviour Policy, staff must never use their personal email addresses or telephone numbers when communicating with students. Should a staff member realise that they have inadvertently communicated in this way, they must report the matter to the DSL immediately.

Publishing images of pupils and their Work
Please refer to *BPS Taking, Storing and Using Images of Children Policy* which in summary states that if parents wish to use their own mobile devices to film pupils at school events:

- They must do considerately, for example without using the 'flash' facility.
- They must make every effort to only record images of their own child, except as part of a group
- They must ensure that any images taken at a school event in which children other than their own appear are not published in any form.
- They adhere to copyright regulations, particularly with respect to School concerts or plays.
- They must not record images in changing rooms or backstage during School productions.
- The above points are also applicable to any adult within the school.

Webcams and CCTV
Staff only use webcams in class for educational purposes. The School operates its CCTV in line with its stated policy.

Misuse and Infringements
All staff have a duty to report breaches of this policy to the *Director of Digital Learning*.

The *Director of Digital Learning* manages all **Online Safety** issues, passing all information available to the *Deputy Head (Pastoral)* or in the case of safeguarding issues on to the *Designated Safeguarding Lead*, copying the Bursar and the Headmaster.

The *Director of Digital Learning* logs all **Online Safety** concerns on the *Online Safety Concerns File*, which the *Deputy Head (Pastoral)* signs termly.

When referred to do so by the *Deputy Head (Pastoral),* the *Director of Digital Learning* will provide training for any students who have transgressed in their use of social media.

The *Director of Digital Learning* and *Deputy Head (Pastoral)* support pupils and staff affected by policy breaches.

The *Deputy Head (Pastoral)* manages all inappropriate or illegal uses of internet, mobile and digital technologies, under the School's behaviour and disciplinary policies. Breaches may also lead to criminal or civil proceedings.

Users of the School system undertake not to visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative);
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative);
- Adult material that breaches the Obscene Publications Act in the UK;
- The promotion of discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status;
- Promote hatred against any individual or group from those protected characteristics listed above;
- Illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy;
- Any material that may bring the School or any individual within it into disrepute e.g., promotion of violence, gambling, libel or disrespect.
- The school follows the recommendations of the 'Sharing nudes and semi-nudes' report: including, teaching within the Computing curriculum of the dangers of such activities, annual staff CPD session covering the issue and creation of a flowchart to identify the process for dealing with an incident should one ever arise. (see Annex B)
- The School treats all inappropriate uses of its systems as disciplinary issues and reserves the right to involve other agencies and authorities, including the Police, in addressing them.

Users of the School system undertake not to:

- Reveal or publicise confidential or proprietary information; Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses;
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the

School;
- Use the School's hardware and Wi-Fi facilities for running a private business;
- Intimidate, threaten or cause harm to others;
- Access or interfere in any way with other users' accounts;
- Use software or hardware that has been prohibited by the School.

Equality
Teaching staff take particular care when undertaking internet activities for children with SEN needs, ensuring that such activities are well-planned, well-managed and that they use additional SEN specific resources as appropriate in lessons.

Please also refer to *BPS Learning Support Policy*.

Parental e-Survey
The *Director of Digital Learning* consults and discusses **Online Safety** with parents / carers annually through an *Online Safety Parent Survey*.

Parental Partnership
The *Director of Digital Learning* disseminates information to parents relating to Online Safety where appropriate in the form of:
- Information sessions
- Posters
- Newsletter items
- Tweets and other social media platforms as appropriate
- Email Notifications
- Informational CDs
- Informational Leaflets.

The *Director of Digital Learning* encourages parents/carers to reinforce the guidance from School when using technologies at home.

END

ANNEX A - Beechwood Park School IT Acceptable Use Policies

Scope and Application of these Policies
Acceptable Use policies apply to all members of the School community, including staff, pupils, parents, and visitors. For the sake of clarity, 'staff' includes teaching and non-teaching staff, pupils, governors, visitors, contractors, sole traders and regular volunteers. 'Visitors' includes anyone else who comes to the School, including parents and occasional volunteers.

Acceptable Use policies apply to pupils and staff accessing the School's technology whether on or off School premises, or using their own, the school's or others technology in a way which affects the welfare of pupils or any other member of the School community or where the reputation of the School is put at risk.

Online behaviour
As a member of the School community you should follow these principles in all of your online activities:

Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.

- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or 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.

Using the School's IT systems
Whenever you use the School's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access School IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access. Do not attempt to install software on, or otherwise alter, School IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT systems, and that the School can view content accessed or sent via its systems.

Passwords
Passwords protect the School's network and computer system and are your 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. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property
Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the *Director of Digital Learning* or the *IT Manager*.

Use of School Systems
The provision of School email accounts, Wi-Fi and internet access is for official School business, administration and education. Staff and pupils 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. Again, please be aware of the School's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely
All official School business must be conducted on School systems, and it is not permissible to use personal email accounts for School business. Any use of personal devices for School purposes, and any removal of personal data or confidential information from School systems - by any means including email, printing, file transfer or cloud - must be registered and approved by the *Network Manager*. Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the School's policies, including two-factor authentication or encryption.

Monitoring and access
Staff, parents and pupils should be aware that School email and internet usage (including through School Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and School email accounts may be accessed by the School where necessary for a lawful purpose - including serious conduct or welfare concerns, extremism and the protection of others. Any personal devices used by pupils, whether or not such use is permitted, may be confiscated and examined under such circumstances. The School may require staff to conduct searches of their personal accounts or devices if they were used for School business in contravention of this policy.

Compliance with related School policies
You will ensure that you comply with the:
- *BPS Online Safety Policy*
- *BPS Anti-Bullying Policy*
- *BPS Child Protection Policy*
- *BPS Data Protection, Record Keeping and Disposal of Records Policy*
- *BPS Health and Safety Policy and Handbook BPS Learning Support Policy*
- *BPS Safeguarding Cause for Concern Record (C4C)*
- *BPS School Trips and Visits Policy*
- *BPS Staff Behaviour Policy*
- *BPS Staff Recruitment Policy*
- *BPS Staff Whistleblowing Policy*
- *BPS Taking, Storing and Using Images of Children Policy*
- *BPS Visiting Speaker Policy*
- *DfE Sexual Harassment and Sexual Violence Advice*
- *Keeping Children Safe in Education September 2021 Part 1*
- *Working Together to Safeguard Children 2018 including Annexe A*
- *Sharing nudes and semi-nudes: how to respond to an incident*

Retention of Digital Data
Staff and pupils must be aware that all emails sent or received on School systems will be routinely kept in archive and email accounts will be closed and the contents deleted within 1 year of that person leaving the School. Important information that is necessary to be kept should be held on the relevant personnel 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 right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol.

If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact the Bursar.

Breach Reporting
The law requires the School 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 School 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 School's systems, e.g. through the use of malware;
- Application of the wrong privacy settings to online systems;
- Misdirected post, fax or email; Sending personal data to an incorrect recipient
- Failing to bcc recipients of a mass email; and Unsecure disposal.

The School generally reports personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether it needs to notify the ICO. If either staff or pupils become aware of a suspected breach, they should contact the *IT Manager*, the Bursar, without delay.

Data breaches will happen to all organisations, but the School takes 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 School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its 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 will be a disciplinary offence.

Breaches of this Policy
A deliberate breach of this policy will be dealt with as a disciplinary matter using the School's usual procedures. In addition, a deliberate breach may result in the School restricting your access to School IT systems. If you become aware of a breach of this policy or the BPS Online Safety Policy, or you are concerned that a member of the School community is being harassed or harmed online you should report it to the Bursar, who will treat reports in confidence.

Acceptance of this Policy
Please confirm that you understand and accept this Online Safety and Acceptable Use policy by signing below and returning the signed copy to the *Director of Digital Learning* who will keep a register of all authorised individuals.

I understand and accept this acceptable use policy (staff / pupils):

Name: …… Signature: …… Date:

……

For younger pupils (below secondary School age)

Name of parent/guardian: …… Signature: …… Date:

……

Annex B

Sharing Nudes and Semi-Nudes (also known as 'sexting')* - how to deal with an incident

What is meant by 'sharing nudes and semi-nudes'?

In the latest advice for schools and colleges (UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online **by** young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's AirDrop which works offline. Alternative terms used by children and young people may include *'dick pics'* or *'pics'*.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated.

This advice does NOT apply to adults sharing nudes or semi-nudes of under 18-year olds.
This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

Steps to follow if an incident comes to your attention

- **Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – this is illegal.**
- Report it to your Designated Safeguarding Lead (DSL) or DDSL **immediately**.
- If you have already viewed the imagery by accident (e.g. if a pupil has shown it to you before you could ask them not to), you **MUST** report this to the DSL or DDSL, who will organise support for you.
- Do **not** delete the imagery or ask the pupil to delete it.
- Do **not** ask the pupil(s) involved in the incident to disclose information regarding the imagery. This is the responsibility of the DDSL.
- Do **not** share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any pupil involved.
- Do explain to the pupil(s) involved that you need to report it and **reassure** them that they will receive support. The member of staff will report to the DSL/DDSL immediately and they will organise appropriate support for the pupil.

*Adapted by D. Buddie from *UK Council for Child Internet Safety* document of the same name