Prebendal School Online Safety Policy

Policy Contents

- Scope of the Policy
- Roles & Responsibilities
- Policy Statements
- Equipment, Filtering & Monitoring
- Responding to Incidents
- Cyberbullying
- Data Storage and Processing
- Appendices
  - Appendix 1 - Acceptable Use Policy for Pupils
  - Appendix 2 - Acceptable Use Policy for Staff
  - Appendix 3 - Resources for parents
  - Appendix 4 - Backup procedures
  - Appendix 5 - Pupil iPad Agreement

SCOPE OF THE POLICY

This policy applies to all members of the Prebendal School community, including staff, pupils, parents and visitors who have access to and are users of school digital technology systems, both in and out of school. In this policy, ‘staff’ includes teaching and non-teaching staff, governors, and regular volunteers. ‘Visitors’ includes anyone else who comes into the school, including occasional volunteers.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school.

Both this policy and the Acceptable Use Policy cover both fixed and mobile internet devices provided by the school, as well as devices owned by pupils, staff, or visitors and brought onto school premises.
The Prebendal School will deal with such incidents within this policy, and associated behaviour and anti-bullying policies, and will, where known, inform parents of incidents of inappropriate Online Safety behaviour that take place out of school.

ROLES & RESPONSIBILITIES

The following section outlines the online safety roles and responsibilities of individuals and groups within The Prebendal School.

The Governing Body

- Is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually.
- The nominated governor for Online Safety is Neville Geake.

The Head and Senior Management Team

- The Head
  o is responsible for the safety of the members of the school community and this includes responsibility for online safety.
  o delegates day-to-day responsibility to the Head of ICT.
- The Head and SMT
  o must ensure that staff, and in particular the Head of ICT, are adequately trained in online safety.
  o must ensure that staff are aware of school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

Head of ICT

- acts as the Online Safety Lead for The Prebendal School, and has undertaken appropriate safeguarding training.
- Should be trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:
  o sharing of personal data.
  o access to illegal or inappropriate materials.
  o inappropriate on-line contact with strangers.
  o potential or actual incidents of grooming.
  o cyberbullying.
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school Online Safety policy.
A5_Online Safety Policy

• ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
• provides training and advice for staff.
• manages and liaises with school technical staff.
• reports regularly to Senior Management Team.
• receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

The Head of ICT is also responsible for ensuring:

• that the technical infrastructure is secure and is not open to misuse or malicious attack.
• that the school meets required online safety technical requirements and any Local Authority Online Safety Policy or Guidance that may apply.
• that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are reviewed regularly.
• that the use of the network, and other technologies provided by the school, is regularly monitored in order that any misuse or attempted misuse can be reported.
• that monitoring software is implemented and updated as agreed in the Acceptable Use policies for Staff and Pupils (Appendix 1 & 2)

All Teaching and Support Staff

Are responsible for ensuring that:

• they have an up to date awareness of online safety matters and of the current Online Safety Policy and practices.
• they have read and understood the Staff Acceptable Use Policy (Appendix 2).
• they report any suspected misuse or problem to the Head of ICT and, where appropriate, the Deputy Head Pastoral (DHP) for investigation.
• online safety issues are embedded in all aspects of the curriculum and other activities.
• pupils understand and follow the Pupil Acceptable Use Policy (Appendix 1).
• pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
• they monitor the use of digital technologies, PCs, iPads, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
• in lessons where internet use is pre-planned pupils should be guided to sites which have been checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

02.09.2019/02.09.2020/DHP/HoICT/M
• are responsible for using the school systems in accordance with the Pupil Acceptable Use Policy (Appendix 1), and for letting staff know if they see the systems being misused.

POLICY STATEMENTS

Education – Pupils

Whilst regulation and technical solutions are recognised as being important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school’s online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience, providing them with the tools to tackle problems as they arise.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned online safety curriculum should be provided as part of PSHE and should be regularly revisited.
• Key online safety messages should be reinforced as part of a planned programme of assemblies and tutor activities.
• Pupils should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
• Pupils should be taught to acknowledge sources of information used and to respect copyright when using material accessed on the internet.
• Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
• Pupils should be helped to understand the need for the Pupil Acceptable Use Policy (Appendix 1) and encouraged to adopt safe and responsible use both within and outside school.
• Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
• Where pupils are allowed to search the internet freely, staff should be vigilant in monitoring the content of the websites that they visit.
Education – Parents & Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children’s online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters & newsletters
- Parental sessions to discuss Online Safety
- High profile events e.g. Safer Internet Day
- Reference to the relevant web sites and publications (see Appendix 3 for resources)

Education & Training – Staff & Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- The Head of ICT will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff at INSET days, led by the Head of ICT.
- The Head of ICT will provide advice or training to individuals as required.

BYOD – Staff & Visitors

Staff at Prebendal are permitted to bring in personal devices for their own use.

These devices include smart phones, tablets, laptops, wearable technology and any similar devices. If you are unsure whether your device is captured by this policy statement, please check with the Head of ICT. These devices are referred to as 'mobile devices' in this policy statement.

Sections one to three and five of this policy statement apply to all school staff and to visitors to the school. The rest of the policy statement is only relevant to school staff.

This policy statement is supported by the Acceptable Use Policy for Staff (Appendix 2).

1. Use of mobile devices at the school

02.09.2019/02.09.2020/DHP/HoICT/M
Staff and visitors to the school may use their own mobile devices in classrooms and common spaces within the school. Staff and visitors to the school are responsible for their mobile device at all times. The school is not responsible for the loss or theft of or damage to the mobile device or storage media on the device (e.g. removable memory card) howsoever caused. The School Office must be notified immediately of any deliberate damage, loss, or theft of a mobile device, and these incidents will be logged.

Mobile devices must be turned off and stored out of sight when in a prohibited area (including the EYFS setting) and/or at a prohibited time and must not be taken into controlled assessments and/or examinations, unless special circumstances apply.

The school reserves the right to refuse staff and visitors permission to use their own mobile devices on school premises.

2. Use of cameras and audio recording equipment

Parents and carers may take photographs, videos or audio recordings of their children at school events for their own personal use.

Other visitors and staff may use their own mobile devices to make photographs, video, or audio recordings in school provided they first obtain permission to take photographs, films or recordings of the relevant individuals. This includes people who might be identifiable in the background.

To respect everyone's privacy and in some cases protection, photographs, video, or audio recordings should not be published on blogs, social networking sites or in any other way without the permission of the people identifiable in them. Parents or carers should avoid commenting on activities involving pupils other than their own in photographs, video, or audio, and other visitors and staff should comment.

No one must use mobile devices to record people at times when they do not expect to be recorded, and devices must not be used that would enable a third party acting remotely to take photographs, video, or audio recordings in school. Staff must comply with the school's social media policy and anti-bullying policy when making photographs, videos, or audio recordings.

3. Access to the school's internet connection

The school provides a wireless network that staff and visitors to the school may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the school, and the school may withdraw access from anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure, and staff and visitors use it at their own risk. In particular, staff and visitors are advised not to use the wireless network for online banking or shopping.
The school is not to be held responsible for the content of any apps, updates, or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

4. Access to school ICT services

Prior to connecting to or accessing school ICT services, mobile devices must be secured with a PIN, password or biometric lock (see section 6 of this policy statement).

School staff are permitted to connect to or access the following school ICT services from their mobile devices:

- the school email system;
- the school’s OneDrive and Sharepoint servers;
- the school servers, via a secure VPN;
- 3Sys.

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for staff to download school information to their mobile devices in order to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it.

Staff must only use the ICT services listed above and any information accessed through them for work purposes. School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Any unauthorised access to or distribution of confidential information should be reported to the Head of ICT as soon as possible.

Staff must not send school information to their personal email accounts.

If in any doubt a device user should seek clarification and permission from the Head of ICT before attempting to gain access to a system for the first time. Users must follow the correct procedures for connecting to the school systems.

5. Monitoring the use of mobile devices

The school may use technology that detects and monitors the use of mobile and other electronic or communication devices which are connected to or logged on to our wireless network or ICT systems. By using a mobile device on the school's ICT network, staff and visitors to the school agree to such detection and monitoring. The school's use of such technology is for the purpose of ensuring the security of its ICT systems, tracking school information.
A5_Online Safety Policy

The information that the school may monitor includes (but is not limited to): the addresses of websites visited, the timing and duration of visits to websites, information entered into online forms (including passwords), information uploaded to or downloaded from websites and school ICT systems, the content of emails sent via the network, and peer-to-peer traffic transmitted via the network.

Staff who receive any inappropriate content through school ICT services or the school internet connection should report this to the Head of ICT as soon as possible.

6. Security of staff mobile devices

Staff must take all sensible measures to prevent unauthorised access to their mobile devices, including but not limited to the use of a PIN, password or biometric lock to be entered to unlock the device, and ensuring that the device auto-locks if inactive for a period of time.

Staff must never attempt to bypass any security controls in school systems or others' own devices.

Staff are reminded to familiarise themselves with the school's relevant policies which set out in further detail the measures needed to ensure responsible behaviour online.

Staff must ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up-to-date.

7. Compliance with Data Protection Policy

Staff compliance with this BYOD policy is an important part of the school's compliance with the Data Protection Act 2018. Staff must apply this BYOD policy consistently with the school's Data Protection Policy.

8. Support

The school takes no responsibility for supporting staff's own devices; nor has the school any responsibility for conducting annual PAT testing of personally-owned devices.

9. Compliance, Sanctions and Disciplinary Matters for staff

Non-compliance with this policy exposes both staff and the school to risks. If a breach of this policy occurs the school will respond accordingly. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on school premises will be temporarily withdrawn. For persistent breach of this policy, the school will permanently withdraw permission to use user-owned devices in school.

10. Incidents and Response

The school takes any security incident involving a staff member's or visitor's personal device very seriously and will always investigate a reported incident. Loss or theft of the
mobile device should be reported to Reception in the first instance. Data protection incidents should be reported immediately to the school's data protection officer.

BYOD – Pupils

Boarders must store their mobile phones with Matron during the school day. Boarders’ access to mobile phones is detailed in BO3_Mobile Phone Policy.

If pupils bring in mobile devices (e.g. for use during the journey to and from school), they must be handed in to the Front Office at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

The school has introduced the use of pupil-owned tablets as a teaching and learning tool and pupils are required to adhere to the Pupil iPad Agreement (Appendix 5) when using tablets for school work, which works alongside, not in place of, the more general Acceptable Use Policy (Appendix 1).

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the SENCo to agree how the school can appropriately support such use. The SENCo, in partnership with the Head of ICT, will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

EQUIPMENT, FILTERING & MONITORING

The school will be responsible for ensuring that the network infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

• School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
• There will be regular reviews and audits of the safety and security of school technical systems.
• Servers, wireless systems and cabling must be securely located and physical access restricted.
• All users will have clearly defined access rights to school technical systems and devices.
• All users in the Prep school will be provided with an individual username and secure password by the Head of ICT who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will normally be required to review their passwords annually.
• Global administrator credentials for the school ICT systems, used by the Head of ICT (and occasionally his deputies) must also be available to Senior Management and kept in a secure place.
• The Head of ICT is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
• Internet access is filtered for all users. Illegal content is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list using a Dell Sonicwall device. Its content lists are regularly updated and internet use is logged and regularly monitored. All changes to the filtering process are undertaken by the Head of ICT.
• Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
• The school has provided differentiated, user-level filtering which only allows pupils and staff to access appropriate content.
• School technical staff regularly monitor and record the activity of users using LanSchool and other software packages on the school technical systems and users are made aware of this in the Acceptable Use Agreements (Appendix 1 & 2).
• Any actual or potential technical incident or security breach must be reported to the Head of ICT and, where appropriate, the Bursar (who acts as the Data Protection Officer).
• Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date anti-virus software.
RESPONDING TO INCIDENTS

Online Safety Incident

- Unsuitable Materials
  - Report to the person responsible for Online Safety
  - If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

- Record details in incident log
- Provide collated incident report logs to LSCB and/or other relevant authority as appropriate

- Review policies and share experience and practice as required
- Implement changes
- Monitor situation

Illegal materials or activities found or suspected

- Illegal Activity or Content (No immediate risk)
- Staff/Volunteer or other adult
- Staff/Volunteer or other adult

- Illegal Activity or Content (Child at Immediate Risk)
  - Report to CEOP

- Secure and preserve evidence

Await CEOP or Police response

- If no illegal activity or material is confirmed then revert to internal procedures
- If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action
Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place through careless or irresponsible use or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority
  - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of ‘grooming’ behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - promotion of terrorism or extremism
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for
safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

**CYBERBULLYING**

Cyberbullying is the use of technology to upset someone else deliberately. It includes:

- threats and intimidation
- harassment
- cyber-stalking
- vilification/defamation
- exclusion or peer rejection
- impersonation
- unauthorised publication of private information or images
- humiliation
- manipulation

**Why is it dangerous?**

- It can be used to carry out all different types of bullying; an extension of face-to-face bullying;
- It can also go further in that it can invade home/personal space and can involve a greater number of people;
- It can take place across age groups and school staff and other adults can be targeted;
- It can draw bystanders into being accessories.

The Prebendal School reserves the right to investigate and deal with any instances of cyberbullying involving members of its community, even when they are off-site and/or out of normal school hours.

**Sexting**

Sexting is the term used to describe the sending of explicit images electronically. This may be via a mobile phone, e-mail or via instant messaging services. Under the Sexual Offences Act (2003) taking an indecent image of a child (someone under the age of 18) is illegal. It is also illegal to send or keep (be in possession of) such an image. This law applies even to a young person taking or sending an image of themselves, and applies to anyone knowingly receiving such an image. Young persons should also advise someone appropriate (an adult) of their actions. Obviously, any sharing of such images is also illegal. There may also be further legal implications if an older pupil requests such pictures of a younger pupil. This could be viewed legally as ‘grooming’.

Pupils should be aware that no data is ever completely erased from a computer or phone – should they ever find themselves the subject of a serious investigation into their ‘online’ behaviour, forensic examination of electronic devices will retrieve all deleted images/texts etc. The main concern about ‘sexting’ is that once an image is sent by a pupil it is then beyond their control.
Sadly, there have been numerous cases of such images then being distributed around and beyond the school community with serious and far-reaching consequences. The requesting of such pictures is not appropriate within our school community. Firstly, it is asking another person to break the law and most importantly because such action does not demonstrate the respect and kindness towards others that is expected. If such behaviour is brought to the attention of the school, the sanction policy will be followed. Sending or distributing such pictures is illegal and will be dealt with accordingly.

This will apply to events both during and outside of term time. This community exists ‘online’ whether we are in school or not.

**PREVENTING CYBERBULLYING**

Understanding and discussion

- The Head of ICT (Deputy Designated Safeguarding Lead) is responsible for overseeing the practices and procedures outlined in this policy and for monitoring its effectiveness, in conjunction with the Deputy Head Pastoral.
- Staff will receive training in identifying cyberbullying and to understand their responsibilities.
- All staff will be helped to keep up to date with the technologies that children are using.
- Pupils are asked to read and sign an acceptable use policy each year and this contains statements regarding cyberbullying.
- Pupils are educated about cyberbullying through a variety of means: in assemblies, anti-bullying week, PSHE lessons, and other projects.

Policies and practices

The Deputy Head Pastoral and Head of ICT will:

- ensure that there are regular reviews and updates of existing policies to include cyberbullying where appropriate;
- keep good records of all cyberbullying incidents;
- publicise rules and sanctions effectively.

Promoting the positive use of technology

- All members of staff will help children to make a positive use of technology across the curriculum;
- The Head of ICT will ensure all staff and children understand the importance of password security and the need to log out of accounts;
- All staff will help the children understand that asking for help is the right thing to do and that it shows strength and good judgement;
• The Head of ICT and DHP will publicise to all members of the school community the ways in which cyberbullying can be reported.

RESPONDING TO CYBERBULLYING

Most cases of cyberbullying will be dealt with through the school’s existing Anti-Bullying Policy (A8_Anti-Bullying Policy) and Behaviour Policy (A4_Behaviour and Sanctions Policy). Some features of cyberbullying differ from other forms of bullying and may prompt a particular response.

The key differences are:

• Impact: the scale and scope of cyberbullying can be greater than other forms of bullying;
• Targets and perpetrators: the people involved may have a different profile to traditional bullies and their targets;
• Location: cyberbullying can take place at anytime and anywhere;
• Anonymity: the person being bullied will not always know who is bullying them;
• Motivation: some pupils may not be aware that what they are doing is bullying; this encourages pupils to join in when they might not normally do so;
• Evidence: unlike other forms of bullying, the target of the bullying may have evidence of its occurrence;
• It is possible that a member of staff may be a victim.

Support for the person being bullied

• The school will offer emotional support and reassure victims that they have done the right thing in coming forward;
• Advise the person not to retaliate or reply;
• Advise the person to consider what information they have in the public domain;
• Unless the victim sees it as a punishment, they may be advised to change their mobile device e.g. mobile phone number;
• If hurtful or embarrassing content is being distributed, the school make reasonable endeavours get it removed from the web. If the person who posted it is known, ensure that they understand why it is wrong and ask them to remove it. Alternatively, contact the host provider and file a report to get the content taken down;
• Confiscate the mobile device, ask pupil to delete the offending content and say who they have sent it to;
• Contact the police in cases of actual/suspected illegal conduct;
• Advise on how to block the person bullying from their sites and services.

Investigation
• Staff and pupils should preserve evidence of cyberbullying by saving phone messages, recording or printing instant messenger conversations, print or produce a screen-grab of social network pages and print whole email messages;
• Any instances of abuse should be reported to the Designated Safeguarding Lead as soon as possible. If inappropriate images are involved the DSL will contact the Local Authority Designated Officer and the Police.

Working with the bully and applying sanctions

The aim of the sanctions will be:

• To help the person harmed to feel safe again and be assured that the bullying will stop;
• To hold the perpetrator to account, getting them to recognise the harm caused and deter them from repeating the behaviour;
• To demonstrate to the school community that cyberbullying is unacceptable and that the school has effective ways of dealing with it, so deterring others from behaving in a similar manner;
• In applying sanctions, consideration must be given to type and impact of bullying and the possibility that it was unintentional or was in retaliation;

Evaluating the effectiveness of prevention measures

• Use Pupil Voice and other appropriate fora to hear the children’s point of view
• Identify areas for improvement and incorporate children’s ideas
• Conduct regular evaluations

Legal duties and powers

• The Head has the power ‘to such extent as is reasonable’ to regulate the conduct of pupils when they are off-site or not under the control or charge of a member of staff. (Education and Inspections Act 2006);
• School staff may request a pupil to reveal a message or other device content and may confiscate a device; they may not search the contents of the device unless the Deputy Head Pastoral or Head agrees and is present with the child;
• Some cyberbullying activities could be criminal offences under a range of different laws including Protection from Harassment Act 1997 and the Communications Act 2003;
• The school reserves the right to investigate and deal with any instances of cyberbullying, involving members of the school community, even when they are off-site.

DATA STORAGE AND PROCESSING

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policies contained in the appendices for further details.
A5 Online Safety Policy

Staff and pupils are expected to save all data relating to their work to the school’s central server using their home folder or the shared drives, or to their OneDrive accounts.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Head of ICT.
The Prebendal School

ICT Acceptable Use Policy for Pupils

At The Prebendal School we encourage children to make use of digital technology for independent learning, research and study, as we recognise that it can help your education. To keep you safe, Mr Pilgrim, and other staff, may monitor your use of the school’s systems, including your emails and web access.

The following rules are designed to keep you safe online. Breaking these rules could result in a temporary or permanent network ban, and may also invoke other sanctions, depending on the situation. Please read the rules and sign to say you have understood them.

Rules:

1. I will only access the school’s computers using my own username and password.
2. I will keep my password a secret and I will not give it to any other person.
3. I will only use digital technology when I have a teacher’s permission.
4. I will only use technology for work and activities approved by the school.
5. I will only email people that I know, or people who my teacher has approved. All messages that I send will be polite and sensible.
6. I will not give my personal details, or anyone else’s, to anyone over the internet.
7. I will ask permission before opening an email or attachment sent by someone that I do not know.
8. I will only use social networking sites which have been approved, with permission and under direct supervision.
9. If I see anything that makes me unhappy or worried, or I receive a message that I do not like, I will switch off the monitor and I will tell a teacher immediately.
10. I agree that the school should check my computer files and emails, and monitor my access to the Internet including the websites that I visit.
11. I will not try to find unacceptable or offensive material on the internet.
12. I will respect copyright and intellectual property.

I have read and I understand The Prebendal School's ICT Acceptable Use Policy:

Name: _________________________________________   Form: __________
Date:____________________________
The Prebendal School

Appendix 2: Staff ICT, Internet and Email Policy

General Statement

To maximise the benefits of its computer resources and minimise potential liabilities, The Prebendal School has adopted this policy. Staff using computers must use these resources responsibly, professionally, ethically and lawfully.

The school has provided access to computer hardware to assist Staff in performing your job. There should not be expectation of privacy in anything the Staff create, store, send, or receive on the school’s computer system. The computer system, network and all workstations belong to The Prebendal School and have been provided for educational purposes. Without prior notice, The Prebendal School may monitor the use of ICT on the school network, review any material created, stored, sent, or received on its network or through the Internet or any other computer network.

Use of computer resources for any of the following activities is strictly prohibited:

- Sending, receiving, downloading, displaying, printing, or otherwise disseminating material that is sexually explicit, profane, obscene, harassing, fraudulent, racially offensive, defamatory, or otherwise unlawful.
- Knowingly disseminating or storing commercial advertisements, solicitations, promotions, destructive programs (that is, viruses or self-replicating code), political information, or any unauthorised material.
- Wasting computer resources by, among other things, sending mass mailings or chain letters, sending excessive amounts of time on the Internet, playing games during working hours, engaging in online chat groups, printing multiple copies of personal documents, or otherwise creating any unnecessary network traffic.
- Using or copying software in violation of a license agreement or copyright.
- Violating any British, European, or international law.

Further detailed information is contained in the following policy statement.

Email and Internet use policy

E-mail provides an excellent means of communication between other staff, outside individuals, and businesses. Use of e-mail both internally and externally over the Internet, however, must be tempered with common sense and good judgment.
To maximise the benefits of this medium and minimise potential liabilities, The Prebendal School has created the following policy and guidelines. Please keep in mind that these are not intended to discourage your use of e-mail in performing your job. Rather, they are intended to ensure that e-mail is used responsibly and with discretion.

Think before sending a message. It is very important to use the same care, courtesy and discretion in drafting e-mail as you would for any other written communication. Anything created or stored on the computer may, and probably will be reviewed by others. Before sending a message, ask yourself the following question: Would I want a judge, jury or the person (s) mentioned to see this message?

**Inappropriate Material**
Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating; defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail. Incoming material of this kind must be reported to the Head of ICT – Do not reply in any way.

**Employee’s duty of care**
Staff should endeavour to make each electronic communication truthful and accurate. You should use the same care and respect for the recipient in drafting e-mail and other electronic documents as you would any other written communication. Please keep in mind that anything stored or created on the computer system may, and likely will, be reviewed by others.

**Duty not to waste computer resources**
Staff must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These include, but are not limited to, mass mailings or chain letters, sending excessive amounts of time on the Internet, playing internet games during working hours, engaging in online chat groups, printing multiple copies of personal documents, or otherwise creating any unnecessary network traffic. Because audio, video and picture files require significant storage space, files of this sort should not be downloaded or sent as e-mail attachments unless they are education related.

**Downloading Software**
Downloading software for installation on the computers is strictly forbidden. Only the Head of ICT or his assistant may perform this action. If you require a special program to assist you in your work, you must ask the Head of ICT to do this for you and he will ensure that the proper licensing agreements are fulfilled.

**Data Protection Implications for Communication**
There are Data Protection implications in the electronic transfer of information and files containing personal information. E-mail is a quick and convenient way to transfer data, but the Data Protection Act governs it in exactly the same way as other computer files. Apply the same qualitative judgement to sending information by e-mail as you would any other means of communication.
A5_Online Safety Policy

Altering attribution information
Staff must identify themselves honestly and accurately when sending e-mail or otherwise communicating by e-mail.

No expectation of privacy
The school has provided access to computer hardware and software to assist you in performing your job. You should not have an expectation of privacy in anything you create, store, send, or receive on the computer system. The computer system, network and all workstations belong to The Prebendal School and have been provided for educational purposes.

Monitoring of computer usage
The Prebendal School has the right to monitor any and all aspects of its computer system including, but not limited to, monitoring sites visited by staff on the Internet, monitoring chat groups and news groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing mail sent and received by users.

Virus Detection
Files obtained from sources outside, including disks brought from home; downloaded from the internet, newsgroups, bulletin boards, or other online services; files attached to e-mail; and files provided by pupils, may contain viruses that could damage the School’s computer network. If you suspect a virus has been introduced onto the network, notify the Head of ICT immediately.

Use of encryption software
Staff may not install or use encryption software on any computer, unless it is approved and installed by the Head of ICT.

Disclaimer of liability for use of the Internet
The Prebendal School is not responsible for material viewed or downloaded by users from the Internet. The internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material.

In general, it is difficult to avoid at least some contact with this material while using the internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the internet do so at their own risk.

External e-mail accounts
External e-mail accounts e.g. Hotmail, Google etc bypass some of the network defences and therefore leave the network vulnerable. All external accounts must be approved by the Head of ICT prior to being accessed. Users will be held liable.
Accessing inappropriate Internet sites
Staff working at The Prebendal School have a duty to conduct themselves in a manner that is appropriate to the culture, aims and objectives of their employer. Deliberate accessing of offensive, pornographic or other inappropriate web sites including social networking sites for personal gratification using School equipment is not in keeping with the nature of their employer. Such activities are likely to be considered as a gross misconduct.

There are occasions when some staff may, in the course of their work, require to access otherwise undesirable web sites. In such cases, the staff involved must clear this in advance in writing with their line manager and also inform the Head of ICT prior to accessing these sites. It is in your own interest to do so.

Blocking inappropriate Internet sites
The Prebendal School may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by staff. However, you may, nonetheless, encounter inappropriate or sexually explicit material while browsing the internet. If you do, immediately disconnect from the site, regardless of whether the site was subject to blocking software, and inform the Head of ICT.

Games and entertainment software
Staff may not use the internet connection to download games or other entertainment software, or to play games over the internet.

Illegal copying
Staff may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licences that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a licence or download any material for which a registration fee is charged without prior consultation with and approval by the Head of ICT. This refers also to copying of CDs without copyright permission.

Data Ownership and Intellectual Property
All files, communications and other data generated as part of or during employment at The Prebendal School shall ultimately remain the physical and intellectual property of the school. Any data created or stored using the school’s systems also remains the property of the school, although individual users are responsible for ensuring that they store data in their control responsibly and securely, in line with Data Protection legislation.
APPENDIX 3 – RESOURCES FOR PARENTS

This appendix contains a non-exhaustive list of resources which parents may wish to use when considering their child’s online safety. Where parents require specific guidance, or have concerns about their child’s online safety at school or at home, they are encouraged to speak with the Head of ICT.

Advice and guidance:

- Internet Matters: https://www.internetmatters.org/advice/
- South West Grid for Learning: https://swgfl.org.uk/products-services/online-safety/resources/
- ThinkUKnow: https://www.thinkuknow.co.uk/parents/
- ChildNet: https://www.childnet.com/parents-and-carers/

Age-appropriate search engines:

- Swiggle (KS2): https://swiggle.org.uk/
- Kiddle (KS2/3): https://www.kiddle.co/

Age-appropriate online encyclopaedias:

- Kiddle Encyclopedia (KS2): https://kids.kiddle.co/
APPENDIX 4 – BACKUP PROCEDURES

At 02:00 each morning an incremental copy of all the files (including the databases of staff, parent and pupil information) on the Prebendal School server(s) is transferred to the Network Attached Storage (NAS) device and a further copy is then made to a cloud storage facility. Therefore, in the case of a server failure the files from the previous close of business are always available from either the NAS or cloud.

During the day, “snapshots” capture changes to our files. These snapshot change records are stored on the NAS device and by reviewing these records the intraday file versions can be recreated.

The backup (on- and off-site) is managed under contract by AlphaScan, a third-party provider. Our data is encrypted before it leaves the site to be stored in the cloud. The ‘cloud’ co-location is with AlphaScan, who hold the encrypted data in Shoreham, West Sussex, within the European Union.

Requests for files to be recovered from backup, or any other issues relating to backup, should be directed to the Head of ICT, who will work with AlphaScan to retrieve the data.
APPENDIX 5 – PUPIL IPAD AGREEMENT

Internet Use

The use of blogs, podcasts and other Web 2.0 applications offer opportunities for you to enhance your learning. Teachers may incorporate email, instant messaging, blogs, podcasts, video sharing, online collaborations, virtual learning environments or other technologies as part of their teaching. However, you must not use any instant messaging or social media at school, unless you have been given express permission to do use by a member of staff (e.g. to access Yammer).

iPads

Year 6, 7 & 8 children may use their own iPads in school for educational purposes, but they must be used responsibly at all times. Power supplies for the devices must not be brought to school; boarders should store their power supplies in the Boarding House - arrangements for charging devices must be made with Boarding staff.

Guidelines:

• Children are responsible for taking care of their device, including any costs of repair, replacement or modifications needed to use the device at school.
• Children are expected to use any mobile device responsibly and appropriately at all times
• Personal mobile devices must not under any circumstances be taken into examination rooms.
• Devices must be stored in the lockable cabinet provided during break times, lunchtimes, and other lessons in which the iPad is explicitly not to be used.
• The school reserves the right to inspect any device if there is reason to believe that a child has violated school policies or rules, or has engaged in other misconduct whilst using the device.
• Misconduct or violations of other policies, e.g. Anti-Bullying Policy, or rules involving a personal device may result in the loss of use of the device and/or further action being taken.
• Use of devices in lessons and form periods is at the sole discretion of the teacher in charge at the time. Any alarms/reminders/chimes etc. must be set to silent whilst in lessons.
• Each child will use only the School’s wireless network and will not physically connect the device to the network.
• The use of VPNs (Virtual Private Networks), proxies (anonymous or otherwise) and/or 3G/4G dongles to get around content filtering is not allowed and neither is the use of peer-to-peer networks to facilitate file sharing/downloading.
  You are not permitted to have a VPN app or profile installed on your iPad.
• Devices must be brought to school fully-charged and must run off batteries during the day. For safety reasons, no attempt must be made to charge the device during the day.
• For safety reasons, devices must not be used in corridors or whilst children are walking between rooms.
• The School accepts no responsibility whatsoever for theft, loss or damage relating to mobile devices. It is the responsibility of parents and children to ensure iPads are safe and properly used.
• Support will be offered by the Head of ICT and other IT staff on a “best efforts” basis and only as time allows.

Signed: _______________________________      Date: _______________________________

Print Name: ________________________________________   Form: _____________________