

Love God, love others

Let your light shine



**THE BLUE COAT CHURCH OF ENGLAND (AIDED) INFANT AND JUNIOR
SCHOOLS' FEDERATION**

INFORMATION SECURITY POLICY

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The Federation is committed to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the Federation to achieve this, including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the Federation of the requirements of information security and the responsibility to staff and all who work for our two schools to protect the confidentiality and integrity of the information that they themselves handle.

Introduction

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Staff are referred to the Federation's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found in the staff shared areas.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is

not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the Federation, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Federation Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment and is not intended to have contractual effect.

Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

General principles

All data stored on our IT systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the Federation's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the Federation ICT Resource Supervisors the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by Federation ICT Resource supervisors or by such third party/parties as the Federation ICT Resource supervisors may authorise.

The responsibility for ensuring the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with Federation ICT Resource supervisors unless expressly stated otherwise. However. All Federation staff have a responsibility for ensuring the security and integrity of all data processed by the Federation.

All staff have an obligation to report actual and potential data protection compliance failures ('data breaches') promptly to the Executive Head who shall investigate the incident. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported promptly to the Data Protection Officer (whose full details can be found in our Data Protection Policy).

Physical security and procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows, on a computer screen, or on papers left on a desk or carried in such a way that personal details can be seen. Computer screens should be locked when the operator moves away, and at the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked cabinets and other storage systems with locks shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards

where there is general access or a risk of general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform Lucinda Adlington, Assistant Head Teacher as soon as possible who will liaise with the Federation Head of Business Strategy. Risk of vandalism or burglary shall be taken into account when assessing the level of security required.

The Federation closes the gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.

CCTV Cameras are in use at various locations.

Visitors must sign in at the reception, being accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

Computers and IT

The Infant or Junior Federation ICT Resource supervisors shall be responsible for the following:

- a) ensuring that all IT Systems are assessed and deemed suitable to comply with the Federation's security requirements;
- b) ensuring that IT Security standards within the Federation are effectively implemented and regularly reviewed, working in consultation with the Federation's management, and reporting the outcome of such reviews to the Federation's management;
- c) in consultation with Lucinda Adlington, Assistant Head Teacher ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules that are in force whether now or in the future, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

Furthermore, the Infant or Junior Federation ICT Resource supervisors shall be responsible for the following:

- a) assisting all members of staff in understanding and complying with this policy;
- b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
- c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate to them, taking into account their job role, responsibilities, and any special security requirements;
- d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing Lucinda Adlington, Assistant Head Teacher, who will liaise with the Data Protection Officer;
- e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
- f) monitoring all IT security within the Federation and taking all necessary action to implement this policy and any changes made to this policy in the future; and
- g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities - Members of staff

All members of staff must comply with all relevant parts of this policy at all times when using the Federation's IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform the Executive Head of any and all security concerns relating to the IT Systems which either could or have led to a data breach as set out in the Breach Notification Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported immediately to the Infant or Junior Federation JCT Resource supervisor as appropriate.

You are not entitled to install any software of your own without the prior approval of the Infant or Junior Federation ICT Resource supervisor. Any software belonging to you must be approved by the Infant or Junior Federation ICT Resource supervisor and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any license agreements to which that software may be subject.

Prior to installation of any software onto the IT Systems, you must obtain written permission by the Infant or Junior Federation ICT Resource supervisor. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Prior to any usage of physical media (e.g. USB memory sticks or disks of any kind) for transferring files, you must make sure the physical media has been virus-scanned. The Infant or Junior Federation ICT Resource supervisor's approval must be obtained prior to transferring files using cloud storage systems.

If you detect any virus this must be reported immediately to the Infant or Junior Federation ICT Resource supervisor (this rule shall apply even where the anti-virus software automatically fixes the problem).

Access security

All members of staff 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.

The Federation has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and protect the Federation's network. The Federation also teaches individuals about e-safety to ensure everyone is aware of how to protect the Federation's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the Infant or Junior Federation ICT Resource supervisor.

All passwords must, where the software, computer, or device allows:

- a) be at least 6 characters long including both numbers and letters;

- b) be changed on a regular basis [and at least every 180 days];
not be obvious or easily guessed (e.g. avoid birthdays or other memorable dates, memorable names, events, or places etc.)
- c) email passwords are to be changed every 90 days.

Passwords must be kept confidential and must not be shared or made available to anyone else unless specifically authorised by a member of the Senior Leadership who will liaise with the Infant or Junior Federation ICT Resource supervisor as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the Federation's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password, you should notify the Infant or Junior Federation ICT Resource supervisor to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary you may write down passwords provided that you store them securely (e.g. in a locked drawer remote from the equipment or device or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a short period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the Federation, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the Federation's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Data security

Personal data sent over the Federation's network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Infant or Junior Federation ICT Resource supervisor who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the Federation's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the Federation's Wi-Fi if you follow the Infant or Junior Federation ICT Resource supervisor's requirements and instructions governing this use. All usage of your own device(s) whilst connected to the Federation's network or any other part of the IT Systems is subject to all relevant Federation Policies (including, but not limited to, this policy). The Infant or Junior Federation ICT Resource supervisor may at any time request the immediate disconnection of any such devices without notice.

Electronic storage of data

All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by Infant or Junior Federation ICT Resource supervisors.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to the Federation or otherwise without prior written approval of the Executive Head. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the Federation's computer network in order for it to be backed up.

All electronic data must be securely backed up by the end of each working day. Remote backups are completed by the Federation ICT Provider and monitored by the Federation ICT Resource Supervisors.

Home working

You should not take confidential or personal or other information home without prior permission of the Executive Headteacher, and only do so where satisfied appropriate technical and practical measures are in place for your journey to and from work and within your home to maintain the continued security and confidentiality of that information.

When you have been given permission to take confidential or other information home, you must ensure that:

- a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
- b) all confidential material that requires disposal is shredded or, in the case of electronical material, securely destroyed, as soon as any need for its retention has passed.
- c) Confidential information must not be left on display or unattended in any vehicle at any time.
- d) Access to any files stored relating to BCF must only be done via the schools VPN and not saved on any personal documents or personal drives.
- e) Any device issued by BCF will be subject to a parental/carer agreement being signed outlining limitations and expectations.

Communications, transfer, internet and email use

When using the Federation's IT Systems you are subject to and must comply with the Federation's Electronic Information and Communication Systems Policy.

The Federation works to ensure the systems protect pupils and staff and are reviewed and improved regularly.

If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the Infant or Junior Federation ICT Resource supervisor.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the school cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email or password protected with the password issued separately, or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the Federation.

Personal or confidential information should not be removed from the Federation's premises without prior permission from the Executive Head teacher except where the removal is both temporary and strictly necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and its confidentiality are maintained. You must ensure that the information is:

- a) not transported in see-through or other un-secured bags or cases;
- b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
- c) not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

Reporting security breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Executive Head teacher. All members of staff have an

obligation to report promptly actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the Executive Headteacher shall, in consultation with Lindsey Harper, Federation Business Manager, immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue. Advice will also be sought as appropriate from the Federation's Data Protection Officer.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Infant or Junior Federation ICT Resource supervisor. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Executive Headteacher.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Business Manager.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Breach Notification Policy.

Related Policies

Staff should refer to the following policies that are related to this information security policy:

- Electronic Information and Communication Systems Policy;
- Data Breach policy;
- Data Protection Policy.