 **ANNEX 1**

**Online Banking Request Form**

School: ……………………………………………………

Bank Account Number: …………………………………………………… Sort Code ……………………………………………………

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name of member of staff** | **Email address** | **Role 1**  Input, authorisation and view of bank transactions | **Role 2**  Authorise and view of bank transactions | **Role 3**  View of bank transactions only | **Role 4**  Input and view of bank  transactions only |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

*(Please mark with an X the role which each individual has approval for)*

Online banking and access rights for the above have been approved by the Governing Body.

All of those listed as *Role 1* and *Role 2* categories are already approved as authorised signatories for the school account.

**Signed**: **Position**: Headteacher **Date:** ..../..…/…....

**Signed:** **Position**: Chair of Governors **Date:** ..../..…/…....

**ANNEX 1**

**Notes**

1. By requesting access to NatWest Bankline, you agree to always abide by the **CONDITIONS OF USE** and **FRAUD AND CORRUPTION RISK** guidance set out further below. NatWest themselves, Schools Finance or MKCC NatWest Bankline system administrators, and Internal Audit, periodically review user activity within the system. Failure to abide by the **CONDITIONS OF USE** will lead to access being **SUSPENDED or REMOVED**, and depending upon the nature of the condition breach, may result in **DISIPLINARY ACTION**.
2. All staff proposed as Role 1 or Role 2 users must already be authorised signatories for the school. If additional signatories are required, then a new school bank mandate form will need to be completed. These are available on the LMS website:

[**https://www.milton-keynes.gov.uk/schools-and-lifelong-learning/information-schools/local-management-schools-lms/banking-including**](https://www.milton-keynes.gov.uk/schools-and-lifelong-learning/information-schools/local-management-schools-lms/banking-including)

1. School governors are **not** permitted to have online access as they are not members of staff of the school or the authority.
2. It is permissible for staff to be set up with both input as well as approval rights as the NatWest online bank facility ensures automated separation of duties, i.e. when inputting an online payment proposal batch a member of staff **cannot** approve that same batch online. They can however approve a batch that someone else has input.
3. It is recommended that the task of inputting payment proposals routinely sits either with the Bursar or appropriate finance staff and **not** with senior members of the teaching staff.
4. Three bank account signatories will, in effect, need to be content with a payment batch before it is processed – one member of staff inputting the payment batch and two members of staff need to approve the transactions. This separation of duties is consistent with the requirements set out in the LMS Scheme for Financing Schools.
5. Once completed and signed a scanned version of the above document should be emailed to [**schoolsfinance@miltonkeynes.gov.uk**](mailto:schoolsfinance@miltonkeynes.gov.uki) to initiate the setup process for online banking.
6. MKCC Treasury can be contacted at [**treasury@milton-keynes.gov.uk**](mailto:treasury@milton-keynes.gov.uk).

**ANNEX 1**

**Conditions of use**

1. Access to NatWest Bankline enables users to access sensitive and confidential financial data only for a work-related purpose and **MUST** be always kept **CONFIDENTIAL**.
2. NatWest Bankline is accessed by Customer ID, User ID, user password and QR code challenge>Smartcard PIN>response code. You should **NEVER SHARE OR DISCLOSE YOUR PASSWORD OR PIN, AND SHOULD KEEP YOUR SMARTCARD SAFE & ACCOUNTED FOR AT ALL TIMES**.
3. From receipt, **YOU ARE RESPONSIBLE FOR THE SAFE KEEPING OF YOUR NATWEST QR READER DEVICE AND BANKLINE SMARTCARD**. You must **KEEP THEM SECURE AT ALL TIMES AND NEVER LEAVE THEM ON SHOW UNATTENDED**.
4. If you enter an incorrect PIN into your QR reader 3 times, the card is **PERMANTELY LOCKED AND CANNOT BE RESET**. The only option is to ask Schools Finance to order you a new card from NatWest which can take up to 10 working days to arrive.
5. If you enter your NatWest Bankline password incorrectly 2 times, you risk your profile being automatically **DISABLED**, so do not attempt again but select the **RESET PASSWORD** option at the foot of the Login screen & you will be emailed an activation code from Bankline to reset.
6. If you enter your NatWest Bankline password incorrectly 3 times, your profile is automatically **DISABLED**. Schools Finance can reinstate your profile upon request, but this may not be actioned immediately.
7. Quarterly reviews of users accessing the system are conducted by Schools Finance and MKCC Treasury and reviewed annually by MKCC Internal Audit:

7i. Any users who have not logged in for **3 MONTHS** will have their profile **SUSPENDED** and they will need to contact Schools Finance to request reinstatement.

7ii. Any **SUSPENDED** users who do not request reinstatement within **6 MONTHS** of suspension will see their profile **DELETED**.

1. It is **YOUR RESPONSIBILITY TO HAND BACK TO YOUR LINE MANAGER YOUR NATWEST QR READER DEVICE AND BANKLINE SMARTCARD** if your role changes and you no longer need access to Bankline or if you are leaving your employment.
2. It is **YOUR LINE MANAGERS RESPONSIBILITY TO INFORM SCHOOLS FINANCE** if your role changes and you no longer need access to Bankline or if you are leaving your employment.
3. You **AGREE TO UNDERTAKE ANY SECURITY OR FRAUD AWARENESS TRAINING** as determined necessary by Schools Finance. Failure to do so will result in your access being **SUSPENDED** or **DELETED**.
4. You **MUST INFORM SCHOOLS FINANCE** if you have any **PAST OR CURRENT FINANCIAL-RELATED CONVICTIONS OR JUDGEMENTS AGAINST YOU** or are being **INVESTIGATED** or have been **SANCTIONED BY A PROFESSIONAL FINANCIAL BODY** for financial misconduct.

**ANNEX 1**

**Fraud and corruption risk**

1. Access to sensitive and confidential information significantly heightens your risk of being targeted for fraud and corruption. If you are approached in any manner and have any doubt at all, **END CONTACT AND REPORT TO SCHOOLS FINANCE, MKCC TREASURY OR MKCC INTERNAL AUDIT IMMEDIATELY**.
2. Fraudsters employ ever-evolving sophisticated techniques, so always be on-guard. If something feels uncomfortable to you or seems too good to be true in any way, **REPORT TO SCHOOLS FINANCE**.
3. You should **NEVER SHARE YOUR LOGIN SECURITY DETAILS WITH ANYONE ELSE**. Passwords and PINs should be kept safe and always held confidentially. If in any doubt, then **CHANGE THEM IMMEDIATELY**.
4. Schools Finance and/or MKCC Treasury and/or NatWest Bankline staff will **NEVER** ask you to divulge your password, PIN or QR response codes over the phone. If in doubt, **TERMINATE THE CALL IMMEDIATLE AND REPORT IT.**
5. Remote and/or home working can lead to complacency around locking your IT device when stepping away from it and/or concealing sensitive information from the view of others not authorised to see it. **YOU ARE REMINDED TO DO SO AT ALL TIMES AND ESPECIALLY WHEN USING NATWEST BANKLINE.**
6. You should not need to print financial records, but should an unlikely need occur, those records should be **HANDLED SENSITIVELY AND CONFIDENTIALLY DESTROYED AS SOON AS THE PURPOSE ENDS**.